الجميع على تواصل
والكل معرّض للخطر
فماذا يمكننا أن نفعل

جرائم المستقبل

FUTURE CRIMES

مارك غودمان



الدار العربية للعلوم ناشرون
Arab Scientific Publishers, Inc.



جرائم المستقبل

FUTURE CRIMES

كل شيء متصل وما من أحد حصين، فما عسانا نفعل؟

everything is connected, everyone is vulnerable and what we can do about it

مارك غودمان

MARC GOODMAN

ترجمة

أحمد حيدر

مراجعة وتحرير

مركز التعريب والبرمجة



الدار العربية للعلوم ناشرون ش.م.ل

Arab Scientific Publishers, Inc. SAL

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيمِ

يتضمن هذا الكتاب ترجمة الأصل الإنكليزي

Future Crimes

everything is connected, everyone is vulnerable and what we can do about it

الطبعة الأولى

1437 هـ - 2016 م

ISBN: 978-614-02-2732-3



تصميم الغلاف: علي القهوجي

مقدمة

المتفائل الطائش: كيف سلكت هذه الطريق

كان دخولي في عالم الجريمة عالية التقانة محض صدفة، عندما كنت أعمل عام 1995 رقيباً محققاً في عمر الثانية والعشرين في مركز شرطة باركر سنتر الشهير التابع لشرطة لوس أنجلوس. فذات يوم، صرخ الملازم باسمي عبر غرفة المحققين المكتظة الصاخبة: "يا غوووددماااان، تعال إليّ هنا!". اعتقدت أنني في ورطة، لكن الملازم طرح عليّ السؤال الذي سيغير حياتي في ما بعد: "هل تعرف كيف تجري تدقيقاً إملائياً في برنامج وورد بيرفيكت؟".

"بالطبع سيدي، ما عليك سوى أن تضغط على مفتاح التحكم مع مفتاح إف – 2"، كان جوابي.

بشّ وجهه وقال: "كنت أعلم أنك الشخص المناسب لهذه القضية".

وهكذا بدأت سيرتي المهنية في شرطة التقانة العالية بالتحقيق في أول جريمة حاسوبية أصادفها. فمعرفة كيفية إجراء التدقيق الإملائي في برنامج لتحرير النصوص وضعني في صفوف النخبة العارفة بالتقانة بين رجال الشرطة في التسعينيات. ومنذ تلك الحادثة صرت مراقباً وتلميذاً دؤوباً لا للتقانة وحسب بل لاستخداماتها المحظورة أيضاً. وعلى الرغم من إدراكي لقدر الأذى والدمار الذي قد يسببه سوء استخدام التقانة، لا تزال تذهلني الطرائق الذكية والمبتكرة التي يتبعها المجرمون لتحقيق مآربهم.

يدأب المجرمون على تحديث تقنياتهم بتطعيم عملياتهم بآخر ما توصلت إليه التقانة. وقد تجاوزوا في تطورهم تلك الأيام التي كانوا فيها أول من يحمل أجهزة البيجر في الشوارع أو حين كانوا يستخدمون الهواتف الخلوية التي يكلف واحدها خمس جنيهات إسترلينية لتبادل الرسائل المشفرة في ما بينهم. فقد باتوا اليوم يبنون نظم الاتصالات الراديوية الخلوية المشفرة الخاصّة بهم وينشرونها في طول البلاد وعرضها، كما تفعل عصابات الناركو

في المكسيك. فلنا أن نتخيل مدى التعقيد الذي يكتنفه نشر شبكة اتصالات مشفرة كاملة الوظائف كهذه على مستوى البلاد. إنه إنجاز مذهل، خصوصاً إذا ما أخذنا في الاعتبار أن كثيراً من الأميركيين حتى يومنا هذا غالباً ما لا تتوفر لهم تغطية خلوية مقبولة.

أثبتت عصابات الجريمة المنظمة أنها سبّاقة إلى تبني التقانة الحديثة، فقد بدأت بشن هجماتها في عالم الشبكات قبل أن تبدأ أجهزة الشرطة بمجرد التفكير بهذه الإمكانية، ولا تزال هذه العصابات محافظة على تفوقها على السلطات في هذا المجال حتى اليوم. فعناوين الأخبار الرئيسية تعج بقصص عن مئة مليون حساب تمت قرصنته هنا، وخمسين مليون دولار سرقت عبر الشبكة هناك. وتطور هذه الجرائم يدعو للصدمة، وهو يتسارع في الاتجاه الخطأ تماماً.

لن يكون موضوع هذا الكتاب ما قد حدث بالأمس أو حتى ما يحدث اليوم، ولن يكون محور تركيزنا هو الطول المناسب الذي عليك اعتماده لكلمة السرّ، بل ما نحن مقدمون عليه في الغد. عبر مسيرة الأبحاث والتحريات التي مررت بها، بدايةً في إدارة شرطة لوس أنجلوس، وخلال عملي اللاحق مع منظمات تنفيذ القانون الاتحادية والدولية، تسنى لي الكشف عن مجرمين تجاوزوا في تطورهم مستوى الجريمة السايبرية كما نعرفها اليوم، فصاروا يعتمدون تقانات جديدة لا تزال ناشئة كالروبوتيات والواقع الافتراضي والذكاء الصنعي والطباعة الثلاثية الأبعاد والبيولوجيا التركيبية. إلا أن زملائي في السلطة التنفيذية والهيئات الحكومية الذين ألتقي بهم في أنحاء العالم، غالباً ما يجهلون هذه التطورات التقانية المضللة، فضلاً عن الاستغلال المتنامي لها من قبل الجريمة المنظمة والمنظمات الإرهابية على حدّ سواء. وبصفتي شخصاً قد كرس حياته للأمن العام والخدمة العامة، يساورني قلق عميق إزاء التوجهات التي أشاهدها

من حولي اليوم.

مع أن البعض قد يتهمني بتأجيج المخاوف أو بالمبالغة في التشاؤم، فإنني أردّ كلا الاتهامين. فقياساً بما شهدته في ما يتعلق بمستقبلنا، أُعتَبَر أقرب إلى المتفائل، بل ربما إلى المتفائل المتهوّر. ولكي أكون واضحاً، أنا لست من محطمي الآلات الجدد، ولم يصل بي الحمق إلى القول بأن التقانة هي مصدر جميع الشرور في العالم. بل على العكس تماماً: إنني أؤمن بالقدرة الهائلة للتقانة التي تؤهلها لأن تكون القوة الدافعة للخير. كما لا بد من أن أنوّه إلى أن ثمة الكثير من الطرق التي يمكن من خلالها استخدام التقانة لحماية الأفراد والمجتمع، وقد سبق أن حدث ذلك غير مرة. لكن التقانة لطالما كانت سيفاً ذا حدّين. وتجاربي في العالم الحقيقي مع المجرمين والإرهابيين، التي شملت ست قارات، قد بينت لي أن قوى الشر لن تتوانى عن استغلال هذه التقانات الناشئة واستخدامها ضد الجماهير. ومع أن الأدلة التي أراها وحدسي يقولان إن مطبات لا يستهان بها تنتظرنا على الطريق، وهي مطبات لم ترصد لها الحكومة أو الصناعة ما يكفي من الموارد لمعالجتها أو محاربتها، فإنني أميل إلى الإيمان باليوتوبيا التقانية التي وعدنا بها وادي السيليكون.

هذا الكتاب هو قصة المجتمع الذي نبنيه بأدواتنا التقانية، وهو يروي كيف يمكن أن تستخدم هذه الأدوات بالذات ضدنا. فكلما وصلنا أجهزتنا وأجزاءً من حياتنا بشبكة المعلومات العالمية، سواءٌ عبر الهواتف النقالة أو الشبكات الاجتماعية وسواءٌ كانت المصاعد، أو السيارات الذاتية القيادة، قل تحصيننا أمام أولئك الذين يعرفون كيف تعمل التقانات المستخدمة وكيف يستغلونها لمصلحتهم أو للإضرار بالمواطن العادي. باختصار، حين يصبح كل شيء متصل، يصبح الجميع أقلّ حصانة. والتقانة التي نتقبلها في حياتنا بشكل اعتيادي دون أية مساءلة أو تمحيص، أو بقليل منهما فقط،

من الوارد جداً أن تعود وتنقضّ علينا.

إنني إذ أسلط الضوء على آخر ما وصلت إليه المعدّات الإجرامية والإرهابية، إنما آمل بإثارة نقاش حيّ كان لا بد منه منذ وقت طويل بين أصدقائي وزملائي في سلك الشرطة والأمن القومي. ومع أن معظم هؤلاء لديهم ما يكفي من هموم الجريمة التقليدية، لا بد لهم، عاجلاً لا آجلاً، من أن يواجهوا التقانات التي تتطور تطوراً أسّياً والتي تجتاحنا كتسونامي محمّل بالمخاطر قادر على زلزلة أمننا العالمي المشترك.

والأهم من ذلك، وبما أنني قد أقسمت منذ وقت طويل على "حماية وخدمة" الآخرين، أودّ أن أتأكد من أن أفراد الخدمة العامة مزودون بالحقائق التي يحتاجون إليها لحماية أنفسهم وعائلاتهم وشركاتهم ومجتمعاتهم من سيل التهديدات القادمة، التي سيكون وصولها أسرع بكثير مما كان متوقعاً. فمن الواضح أن حصر هذه المعارف بأشخاص "داخليين" يعملون في الحكومة والأمن وفي وادي السيليكون لن يجدي نفعاً.

طوال فترة عملي في الخدمة العامة، حيث عملت مع أجهزة مثل شرطة لوس أنجلوس والإف.بي.آي والاستخبارات الأميركية والإنتربول، كان يتضح لي على نحو متزايد أن المجرمين والإرهابيين كانوا يبزون بابتكاراتهم قوات الأمن في جميع أنحاء العالم وأن الطيبين يتخلفون عن الركب أكثر فأكثر. وسعياً إلى تحقيق أثر أكبر على الجحافل المتنامية من المجرمين الذين يستخدمون أحدث التقانات، غادرت القطاع الحكومي وانتقلت إلى وادي السيليكون لكي أستزيد علماً حول ما هو قادم.

وفي كاليفورنيا، انغمست في وسط من المبدعين التقانيين لكي أتفحص أثر آخر اكتشافاتهم العلمية على المواطن العادي. فزرت معاقل وادي السيليكون، وعقدت الصداقات في أوساط الشركات الناشئة الموهوبة في

منطقة خليج سان فرانسيسكو. ودعيت للانضمام إلى كوادر جامعة سينغولاريتي، تلك المؤسسة المدهشة القائمة في حرم مركز أبحاث إيمس التابع لوكالة ناسا، حيث عملت مع لفيف من اللامعين من رواد الفضاء وعلماء الروبوتيات والبيانات والحواسب وعلماء البيولوجيا التركيبية. يتمتع هؤلاء الرواد، رجالاً ونساءً، بالقدرة على رؤية ما وراء عالم اليوم، مما يفتح آفاقاً هائلة للتقانة تمكّنها من مواجهة أعتى التحديات التي تقف في وجه الإنسانية.

إلا أن الكثير من رجال أعمال وادي السيليكون هؤلاء، الذين يعملون بجد لخلق مستقبلنا التقاني، لا يولون كبير اهتمام للمصلحة العامة أو للمخاطر القانونية والأخلاقية والأمنية التي تفرضها إبداعاتهم على بقية المجتمع. وتجربتي الشخصية في تكبيل المجرمين بالأصفاد والعمل مع قوات الشرطة في أكثر من سبعين بلداً، خلّفت لدي وجهة نظر مختلفة حول إساءة الاستخدام المحتملة للتقانات الناشئة، التي غالباً ما يرحب الأبرياء في كل مكان بدخولها إلى حياتهم اليومية دون مساءلة.

لهذه الغاية، أسّست معهد جرائم المستقبل، حيث كان الهدف هو استغلال تجاربي الخاصة كشرطي ميداني ومحقق ومحلل دولي لمكافحة الإرهاب، وهو الأهم، كشخص من داخل وادي السيليكون، لأحضّ على تأليف جماعة من الخبراء المتوافقين في العقلية لمعالجة الآثار، السلبية منها والإيجابية، لتقانة تتطور سريعاً.

حين أتأمل مستقبلنا، تزداد مخاوفي حيال الانتشار المطلق للحوسبة في حياتنا. فاعتمادنا الكلي عليها يتركنا ضعفاء من نواحٍ قلّ جداً من يستطيع مجرد التفكير بها. فتشكيلات النظم الحالية واعتمادها بعضها على بعض في نمو مستمر. إلا أن ثمة أفراداً ومجموعات على إدراك بأبعاد هذا النمو وسرعته، وهم يواكبونه بإبداعاتهم التي ترمي إلى إلحاق الأذى بنا جميعاً.

هذه هي قصتهم، قصة الجريمة المنظمة والقراصنة والحكومات المارقة، والفاعلين المحليين، والإرهابيين، الذين يتنافسون جميعاً لاستغلال أحدث التقانات لمصلحتهم الخاصة.

إن اليوتوبيا التقانية التي يعد بها وادي السيليكون قد تكون ممكنة، لكنها لن تظهر بقدرة قادر من ذاتها. فعلى المواطنين والحكومات والشركات والمنظمات غير الحكومية أن تقدم قدراً هائلاً من الاهتمام وأن تبذل جهوداً جبّارة وتناضل من أجل تحقيق الثمار المرجوة. فقد نشبت معركة جديدة بين أولئك الذين يريدون الاستفادة من التقانة لمصلحة الإنسانية وأولئك الذين يفضلون تخريب هذه الأدوات مهما كان الضرر الذي سيلحق بالآخرين. إنها معركة من أجل روح التقانة ومستقبلها، وهي تستعر في الخلفية، محاطة بسرية كبيرة، وهي بالتالي خفيةٌ تماماً على المواطن العادي.

متجاوزاً مجرد تصنيف آخر الابتكارات الإجرامية ونقاط الضعف التقانية، يعبّد هذا الكتاب الطريق لمكافحة التهديدات الكثيرة التي تنتظرنا. فالبصيرة المتيقظة، على ما أرى، ستمكننا من توقع جرائم الغد ومنعها منذ اليوم، قبل أن نصل إلى نقطة اللاعودة. وأجيال المستقبل ستنظر إلى الخلف وتحكم على الجهود التي نبذلها اليوم للحد من هذه التهديدات الأمنية والدفاع عن روح التقانة لضمان أن تصبّ في النهاية في صالح البشرية.

وأخيراً تحذير من صديق: إذا تابعت قراءة الصفحات التالية، فلن تنظر بالطريقة نفسها إلى سيارتك أو هاتفك الذكي أو مكنستك الكهربائية مرة أخرى.

إنها فرصتك الأخيرة. بعد ذلك، ما من عودة. فحين تأخذ الحبة الزرقاء، تنتهي القصة وتصحو في سريرك معتقداً ما تشاء. أما إذا أخذت الحبة الحمراء، فستبقى في بلاد العجائب، وسأريك حينها العمق الذي يصل

إليه جحر الأرنب. وتذكر، كل ما لدي لأقدمه هو الحقيقة، ولا شيء سوى الحقيقة.

مورفيوس محذراً نيو، فيلم المصفوفة (ماتريكس)

الجزء الأول هدوء ما قبل العاصفة

الفصل الأول

اتصال، تبعية، هشاشة

التقانة...شيء خبيث، تمنحك هبات عظيمة بيد وتطعنك في ظهرك باليد الأخرى.

تشارلز بيرسي سنو

كانت حياة ماتّ هونان تبدو في أحسن حال على الشاشة، فعلى إحدى صفحات متصفحه كانت صور طفلته الرضيعة، بينما تسرد صفحة أخرى تغريدات كتبها الآلاف من متابعيه على تويتر. كان المحرر في مجلة وَيَرْد في سان فرانسيسكو يعيش حياةً مدنية تواصلية، أما من ناحية التقانة، فلم يكن يقلّ عن غيره متابعة. إلا أنه لم تكن لديه أدنى فكرة بأن عالمه الرقمي برمّته قد يصبح أثراً بعد عين، بمجرد أن تُضغط حفنة من المفاتيح. لكن ذلك ما حدث في أحد أيام آب. ففي ذلك اليوم، وقعت صوره ورسائل بريده الإلكتروني وأشياء أخرى كثيرة بين يدي قرصان. وفي غضون بضع دقائق فقط، قام مراهق في الطرف الآخر من العالم بسرقتها. لقد كان هونان هدفاً سهلاً، مثلنا جميعاً.

يتذكر هونان ذلك العصر الذي تداعى فيه كل شيء. فقد كان يلعب على الأرض مع طفلته الرضيعة، عندما نفدت طاقة هاتف الآيفون فجأة. ربما تكون بطاريته قد عطبت، لكنه كان ينتظر مكالمة هامة، فوصل الهاتف بالمقبس وأعاد تشغيله. وبدلاً من شاشة الإقلاع والتطبيقات المعتادة، وجد أمامه شعار أبل الأبيض كبيراً وشاشة ترحيب متعددة اللغات تدعوه لإعداد هاتفه. كان أمراً غريباً، لكن هونان لم يساوره كبير قلق: فقد اعتاد إجراء نسخة احتياطية لهاتفه كل ليلة. أما خطوته التالية فكانت واضحة تماماً: تسجيل الدخول على آي.كلاود واستعادة برمجيات وبيانات الهاتف. وعندما حاول تسجيل الدخول باستخدام حساب أبل الخاص به، تم إعلامه

بأن كلمة السر، التي كان متأكداً من صحتها، قد اعتبرت خاطئة من قبل آلهة الآي.كلاود. لكن هونان، المراسل الذكيّ لأهم مجلة تقانة في العالم، كانت لا تزال في جعبته حيلة أخرى. فكل ما كان عليه فعله هو أن يصل هاتفه بحاسبه المحمول ليستعيد البيانات من القرص الصلب على حاسبه المحلي. لكن ما حدث بعد ذلك جعل قلبه ينفطر.

فما إن شغّل هونان حاسب الماك الخاص به، حتى طالعته رسالة من برنامج التقويم من أبل تقول إن كلمة سر الجيميل لديه ليست صحيحة. وبعد ذلك مباشرة، تغير وجه الحاسب، تلك الشاشة الجميلة، فأصبح شاحباً وصامتاً، وكأنه قد مات. وكان الشيء الوحيد الذي يمكن رؤيته على الشاشة هو رسالة: يرجى إدخال كلمة السر المكونة من أربعة أرقام. وكان هونان يعلم أنه لم يضع كلمة سر على الإطلاق.

علم هونان في نهاية المطاف أن المهاجم قد تمكن من الدخول إلى حسابه على آي.كلاود، ثم استخدم ميزة "العثور على الهاتف النقال" لتحديد مواقع جميع الأجهزة الإلكترونية في عالم هونان، ليخترقها جهازاً تلو الآخر. ثم أصدر المهاجم أمر "حذف عن بعد" لمحو جميع البيانات التي أمضى هونان عمره في جمعها. وبعد هاتف الآيفون الذي كان أول الضحايا جاء دور جهاز الآيباد اللوحي. وأخيراً وليس آخراً، وصل الهجوم إلى الحاسب المحمول. في ومضة عين، تم تدمير جميع البيانات، بما فيها كل صورة التقطها لرضيعته في سنتها الأولى. كما ضاعت أيضاً صور لا تقدر بثمن لأقاربه المتوفين منذ زمن بعيد، فذرتها يد مجهولة ذرّ الرياح.

ثم حان وقت الإجهاز على حساب هونان على غوغل. ففي لمح البصر ضاعت جميع رسائل البريد الإلكتروني التي كان قد اعتنى بها على مدى ثماني سنوات. وبنقرة من الفأرة، حذفت محادثات العمل والملاحظات ورسائل التذكير والذكريات. وأخيراً تفرغ المهاجم لهدفه النهائي: حساب

هونان على تويتر MAT@. ولم يكتف المهاجم بالاستيلاء على الحساب، بل إنه استخدمه ليبث تصريحات عنصرية باسم هونان ليقرأها الآلاف من متابعيه.

بعد الهجوم الرقمي وظف هونان قدراته كمراسل تحقيقات لكي يعيد بناء سير الأحداث. فاتصل بالدعم التقني لشركة أبل لاستعادة حسابه على آي.كلاود. وبعد تسعين دقيقة على الهاتف، علم هونان أنه هو "شخصياً" كان قد اتصل قبل ثلاثين دقيقة طالباً إعادة تهيئة كلمة السر. واتضح له أن كل ما يحتاج إليه المرء ليطلب إعادة تهيئة كلمة مروره هو عنوان الفوترة الخاص به، وهو عنوان متاح في سجله على مجال هو.إز للتعريف بالأفراد على الإنترنت، الذي كان قد أنشأه عندما أعدّ موقعه الشخصي. وحتى لو لم يكن هذا العنوان متاحاً هناك، فإن العشرات من الخدمات الشبكية، مثل خدمة الصفحات البيضاء وموقع سبوكيو، كانت ستقدمه بالمجان.

وللتحقّق من الخانات الأربع الأخيرة من بطاقة ائتمان هونان، خمّن المهاجم أن يكون لدى هونان، مثل كثيرين، حساب على موقع أمازون، وقد أصاب في ذلك. فبعد أن تسلح باسم هونان الكامل وعنوان بريده الإلكتروني وعناوينه البريدية، اتصل المجرم بموقع أمازون ونجح في خداع ممثل خدمة الزبائن فيه، بحيث جعله يعطيه الخانات الأربع من رقم بطاقة الائتمان. وكانت هذه الخطوات البسيطة كافية لقلب حياة هونان رأساً على عقب. بل إنه كان بإمكان المهاجم، وإن لم يفعل ذلك هذه المرة، بكل بساطة أن يستخدم هذه المعلومات نفسها للوصول إلى حسابات هونان في المصرف وفي سوق الأسهم ويسرق محتوياتها.

ثم ظهر أخيراً المراهق الذي قام بالهجوم للافتخار بفعلته (وكان معروفاً في أوساط القراصنة باسم فوبيا)، مدعياً أنه سيقوم بالكشف عن الكثير من نقاط الضعف الأمنية في خدمات الإنترنت، التي نعتمد عليها جميعاً في

حياتنا اليومية، وهو ما حققه بالفعل. وأنشأ هونان حساب تويتر جديداً للتواصل مع مهاجمه. ووافق فوبيا، مستخدماً حساب ماتّ المسلوب، على متابعة حساب هونان الجديد، فأصبح بإمكان الاثنين أن يتبادلا الرسائل في ما بينهما مباشرة. وطرح هونان على فوبيا السؤال الوحيد الذي كان يفترسه: "لماذا؟ لماذا تفعل بي هذا؟". ليكتشف بعد ذلك أن بيانات وذكريات عقد كامل قد ضاعت كمجرد ضرر جانبي.

فقد جاءت إجابة فوبيا الباردة: "بصراحة، لم أكن أُكِنّ لك أي حقد...كل ما في الأمر أن اسم حسابك على تويتر قد أعجبني". هذا كل ما في الأمر. كل ما هنالك هو حساب تويتر ثمين أعجب مهاجماً مقيماً على بعد آلاف الأميال فأراده ببساطة لنفسه.

ربما كان سخيفاً أن يكون بإمكان شخص لا يكنّ لك أيّ "شعور"، أن يضغط على بضعة مفاتيح ليمحو حياتك الرقمية. عندما ظهرت قصة هونان على غلاف مجلة ويرد في كانون الثاني عام 2012، نالت قدراً كبيراً من الاهتمام... لدقيقة أو دقيقتين. واندلع الجدل في طريقة تأمين تقاناتنا اليومية بطريقة أفضل، مثل كثير من النقاشات على الإنترنت، لكن جذوة هذا النقاش سرعان ما انطفأت. وما تغير منذ محاولات ومحن هونان قليل وثمين في آن معاً، فنحن لا نزال ضعفاء تماماً كما كان هونان وقتئذ، وربما أكثر منه، مع ازدياد اعتمادنا على تطبيقات نقالة وسحابية قابلة للاختراق.

كما هي الحال لدى معظمنا، كانت حسابات هونان المختلفة مرتبطة ببعضها بشبكة من الإحالات الذاتية للثقة الرقمية المزعومة: فرقم بطاقة الائتمان نفسه يستخدم على حساب أبّل وفي موقع آمازون، وحساب آي.كلاود الإلكتروني يشير مجدداً إلى حساب الجيميل. وكانت ثمة معلومات مشتركة، منها بيانات تسجيل الدخول وأرقام بطاقات الائتمان وكلمات السر، وكانت جميع هذه البيانات تشير إلى الشخص نفسه. فلم تكن

الحمايات الأمنية لدى هونان أكثر من مجرد خط ماجينو رقمي، مجرد بيت من الورق لم يلبث أن انهار حين هبّ النسيم. فجميع أو معظم المعلومات اللازمة لتدمير حياته الرقمية، أو حياتك أنت، متوفرة على الشبكة ويمكن لأي شخص أن يحصل عليها إذا ما تمتع ببعض المكر أو الإبداع.

التقدم والمخاطر في عالم متشابك

في غضون بضعة أعوام، ومع القليل جداً من التأمل، استطعنا أن ننتقل من مجرد البحث عبر غوغل، إلى الاعتماد عليه في تحديد الاتجاهات وإدارة التقاويم ودفاتر العناوين ومشاهدة الفيديو، وفي الترفيه والبريد الصوتي والاتصالات الهاتفية. وثمة مليار شخص بيننا يقومون بنشر أكثر تفاصيل حياتهم حميمية على فايسبوك ويقدمون طواعية خرائط شبكاتهم الاجتماعية، المشتملة على العائلة والأصدقاء وزملاء العمل. لقد قمنا بتنصيب مليارات التطبيقات التي نعتمد عليها في تنفيذ كل شيء، من الصيرفة والطبخ إلى أرشفة صور أطفالنا. أما اتصالنا بالإنترنت، فنجريه عبر حواسبنا المحمولة وأجهزة الهاتف النقالة والحواسب اللوحية وأجهزة تسجيل البث التلفزيوني (التيفو)، ومستقبلات البث السلكي ومنصات ألعاب بي.إس.3 وأجهزة البلوراي والنينتيندو وأجهزة التلفاز العالية الدقة ومشغّلات الروكو للفيديو وتلفزيونات أبل.

جلية هي إيجابيات الثورة التقنية، فعلى مدى السنوات المئة الأخيرة، أدّت التطورات المتسارعة في العلوم الطبية إلى ارتفاع متوسط العمر البشري إلى أكثر من الضعف، وانحسرت وفيات الأطفال إلى العُشر. أما متوسط دخل الفرد، فتضاعف ثلاث مرات على مستوى العالم. وصار التعليم عالي الجودة في متناول الجميع اليوم عبر مواقع على الوب، مثل أكاديمية خان، بعد أن كان حلماً صعب المنال بالنسبة لكثيرين. وتفرّد الهاتف النقال بكونه صاحب الفضل في تدفق المليارات من الدولارات، في تنمية اقتصادية

مباشرة في جميع دول الأرض.

بفضل الاتصالات التي توفرها الإنترنت عبر بنيتها الثورية، بات ممكناً لشعوب العالم أن تلتقي على نحو لم يسبق أن كان ممكناً بعد أن كانت معزولة بعضها عن بعض. فيمكن لسيدة في شيكاغو أن تلعب لعبة "كلمات بين الأصدقاء" مع شخص غريب عنها تماماً يقيم في هولندا. ويمكن لطبيب في مقاطعة بانغالور في الهند، أن يطّلع على نتائج تصوير أشعة لمريض في مدينة روكا راتون في فلوريدا ويفسر محتواها. ويستطيع مزارع في جنوب أفريقيا أن يستخدم هاتفه النقال للوصول إلى بيانات المحاصيل، مثله في ذلك مثل طالب دكتوراه في معهد ماساتشوستس للتقانة. إن إمكانيات الاتصال البينية هي إحدى أعظم نقاط قوة الإنترنت، وهي في تعاظم مستمر، تواكبها قوة الشبكة العالمية ومنافعها. فثمة الكثير مما يجدر الاحتفاء به في عالمنا التقاني الحديث.

بينما يجري توثيق وإبراز منافع العالم الشبكي بعناية من قبل أولئك الذين يعملون في صناعة التقانة، فإن لهذه التواصلية جانبها المظلم أيضاً.

فشبكات الكهرباء وشبكات التحكم بالملاحة الجوية ونظم توزيع أقسام الإطفاء، بل وحتى المصاعد في الشركات لدينا، جميعها تعتمد اعتماداً هائلاً على الحواسب. مع مرور كل يوم، نقوم بوصل المزيد والمزيد من جوانب حياتنا اليومية بشبكة المعلومات العالمية، دون أن نتوقف لنتساءل عن مغزى كل ذلك. كانت تجربة ماتّ هونان قاسية، وكذلك تجارب الآلاف غيره. لكن ما الذي يفترض أن يحدث إذا، أو عندما، تزول جميع هذه الحيل التقانية التي يعتمد عليها مجتمعنا الحديث اعتماداً مطلقاً؟ ما هي الخطة الاحتياطية للبشرية؟ في الحقيقة، ما من خطة حاضرة.

العالم مسطح (ومفتوح على مصراعيه)

ساد النظام الغربي الفيستفالي للدولة - الأمة السيادية عالمنا لقرون

طويلة. وهو يعني أن للبلدان سيادتها على مناطقها التي ليس لأي قوة خارجة أن تتطفل فيها على شؤون الأمة المحلية. وكانت البنية الفيستفالية تتحصن بنظام من الحدود والجيوش والحرس والبوابات والأسلحة. وكان ممكناً فرض القيود للحد من الهجرة الداخلة والخارجة إلى ومن أراضي الأمة. علاوة على ذلك، كانت تقام هيئات الجمارك والتفتيش للسيطرة على تدفق البضائع عبر الحدود الوطنية. لكن على الرغم من البصيرة التي كان يتمتع بها الموقعون على اتفاقية فيستفاليا عام 1648، فإنهم لم يتوقعوا ظهور سناب شات.

مع أنه لا تزال للحدود المادية أهميتها، فإن مثل هذه التقسيمات باتت أقل وضوحاً في العالم الشبكي. فالبتات والبايتات تتدفق بحرية من بلد إلى آخر دون حرس حدود وإدارة هجرة أو تصريحات جمركية تبطئ تنقلها. والحواجز الدولية التقليدية التي كانت تقف في وجه الجيل السابق من اللصوص والعصابات وأصحاب السوابق، دمّرت في العالم الشبكي الذي بات يسمح للمنحرفين بدخول ومغادرة أي موقع افتراضي يختارونه بكل حرية.

لنتأمل مضاعفات ذلك على مجتمعنا. فذات يوم، كانت أشياء عديدة تعتبر بديهية حين يحاول مجرمون السطو على بنك في ساحة التايمز في مدينة نيويورك. فأولاً وقبل كل شيء، كان يفترض أن المهاجمين قد دخلوا موقعاً مادّياً يقع ضمن حدود صلاحية قسم شرطة نيويورك في جنوب وسط المدينة. وكانت عملية سطو كهذه ستمثل انتهاكاً لقانون ولاية نيويورك وللقوانين الأميركية الفدرالية في آن معاً، ما كان سيمنح قسم شرطة نيويورك ومكتب التحقيقات الفدرالية صلاحية مشتركة للتحقيق في القضية. أما الضحية (أي المصرف في هذه الحالة)، فتقع أيضاً في النطاق القضائي المادي للسلطات التنفيذية المعنية، ما يسهل التحقيقات إلى حد كبير. وكانت محاولات حل القضية ستستند إلى أدلة مادية، من المرجح أن يكون

مهاجمو المصرف قد خلفوها وراءهم، مثل بصمات أصابع متروكة على ورقة سلمت إلى محاسب المصرف أو آثار دي.إن.إي متروكة على منضدة قفز عنها أحد المهاجمين، بل وربما صورة لوجهه التقطتها إحدى الكاميرات الأمنية. علاوة على ذلك، تبقى مثل هذه الجريمة محدودة بقيود مادية معينة. فالأوراق النقدية المسروقة سيكون لها وزن وحجم يجعلان العدد الممكن حمله منها محدوداً. وربما تكون رزم الدولارات مزوّدة بحزام دبغة متفجرة يفضح المشتبه بهم أمام الشرطة. أما في عالم اليوم، فإن البديهيات الجنائية التي لطالما كانت سليمة ومجرّبة، مثل ميزات الصلاحية القضائية والأدلة المادية، والتي تُعدّ أدوات أساسية تساعد السلطات على حل الجرائم، لم تعد موجودة في أغلب الأحيان.

يمكننا أن نقارن بين سيناريو عملية السطو في ساحة التايمز المشار إليها آنفاً، بعملية السطو الشبكية الشهيرة التي قام بها فلاديمير ليفين عام 1994 من شقته في سانت بيترسبورغ في روسيا. فقد اتُّهم ليفين، وهو مبرمج حاسوب، بانتهاك حسابات العديد من كبار الزبائن التجاريين لمصرف سيتيبانك، والهروب بمبلغ 10.7 ملايين دولار. وكان ليفين، متعاوناً مع شركاء له في أنحاء العالم، قد حوّل مبالغ ضخمة من الأموال إلى حسابات في فنلندا والولايات المتحدة وهولندا وألمانيا وإسرائيل.

فمن يمتلك الصلاحية القضائية للبت في هذه القضية؟ شرطة الولايات المتحدة الأميركية، حيث يقع المصرف الضحية؟ أم شرطة سانت بيترسبورغ، حيث نفذ المشتبه بهم اعتداءهم المفترض؟ أم إن الصلاحية القضائية ربما تقع في إسرائيل أو فنلندا، التي حولت إليها مبالغ طائلة من الأموال الإلكترونية لتحط في حسابات احتيالية. لم يسبق لليفين أن دخل الولايات المتحدة مادياً ليقترف جريمته. وهو لم يخلف وراءه أية بصمات أو آثار دي.إن.إيي، كما لم تعلّم عليه أية صبغة متفجرة. والأهم من ذلك أنه لم

يضطر أساساً لحمل آلاف الباوندات من الأموال مادّياً والخروج بها من المصرف، بل قام بما قام به بواسطة الفأرة ولوحة المفاتيح، فلم يكن مضطراً لاستخدام قناع ولا بندقية معدّلة يدوياً، بل كان عليه فقط أن يجلس وراء شاشة الحاسب ويستخدم مساراً افتراضياً متشعباً لتغطية تحركاته الرقمية.

تجعل الإنترنت بطبيعتها عالمنا الذي نعيش فيه مع مرور الوقت عالماً بلا حدود. فبإمكان أي شخص اليوم، سواء كان مقصده خيراً أم شراً، أن يسافر بسرعة الضوء إلى الطرف الآخر من العالم. لقد جاءت التقانة نعمةً على المجرمين الذين يتنقلون من بلد إلى آخر مخترقين طريقاً لهم افتراضياً عبر الكوكب، موصلين الشرطة إلى حد القنوط. كما أن المجرمين قد تعلموا كيف يحمون أنفسهم من التتبع عبر الشبكة، فالمهاجم الذكي لن يشن هجوماً على مصرف في البرازيل في أي حال من الأحوال مباشرةً من شقته في فرنسا. بل سيحوّل هجومه من شبكة مخترقة إلى أخرى، من فرنسا إلى تركيا إلى المملكة العربية السعودية، إلى أن يصل هدفه النهائي في البرازيل. وهذه القدرة على القفز بين البلدان، والتي تعد من أعظم نقاط قوة الإنترنت، تخلق للشرطة مشكلات قضائية وإدارية هائلة وهي أحد أسباب صعوبة التحقيقات في الجرائم السايبرية، بل وعقم هذه التحقيقات في أغلب الأحيان. فليس لضابط شرطة في باريس صلاحية إلقاء القبض على شخص في ساو باولو.

سقى الله أيام الجريمة السايبرية

تغيرت طبيعة التهديدات السايبرية تغيراً جذرياً خلال السنوات الخمس والعشرين المنصرمة. ففي الأيام الأولى للحاسب الشخصي، كان أكثر ما يحفز المهاجمين هو التهليل والضحك. فكانوا يخترقون نظاماً حاسوبياً لمجرد أن يثبتوا أن باستطاعتهم فعل ذلك أو ليثبتوا وجهة نظر ما. وقد كان أحد أول الفيروسات الحاسوبية التي أصابت حواسب آي.بي.إم الشخصية هو فيروس

برين (الدماغ)، الذي صنعه الأخوان أمجد فاروق ألفي وباسط فاروق ألفي، اللذان كانا في الرابعة والعشرين والسابعة عشرة، من لاهور في الباكستان. وكان الغرض من فيروسهما حميداً، إذ كانت مهمته منع الآخرين من قرصنة البرمجيات التي كان الأخوان قد أمضيا سنوات في تطويرها. فقد قام الأخوان، وقد أزعجتهما قرصنة الآخرين لبرمجياتهما من دون دفع ثمنها، بتضمين هذه البرمجيات تحذيراً شديد اللهجة يقول:

أهلاً بك في دونجيون برين وأمجد

(العنوان والهاتف) احذر هذا الفيروس واتصل بنا لمعالجته

كانت رسالتهما هذه هامة لعدة أسباب. أولها أن الأخوين قد ادعيا حمل الحقوق الفكرية لفيروسهما، وهو كلام لا معنى له. والأغرب من ذلك هو أنهما ضمّنا عنوانهما وأرقام هاتفيهما، بحيث يتسنى للمستخدمين الاتصال بصانعي الفيروس من أجل "معالجته" أو إزالته. بدت أسباب صنع الفيروس وجيهة بما يكفي بالنسبة لباسط وأمجد، لكن ما لم يدركاه هو أن المخلوق الذي صنعاه كان قادراً على الانتساخ والانتشار بالطريقة التقليدية، أي عبر بشر يحملون أقراصاً مرنة قياس 5.25 إنش وينقلونها من حاسب إلى آخر. وفي نهاية المطاف، تنقل فيروس برين عبر المعمورة معرفاً بقية العالم بباسط وأمجد.

لم يزدد المهاجمون مع الوقت إلاّ طمعاً وخبثاً، فاتصالنا بعضنا ببعض عبر نظم خدمات الشبكات الحاسوبية، يعني أنه لم يعد على الفيروسات أن تنتقل عبر "أشراك تسللية" يحملها البشر على أقراص مرنة، بل يمكنها الانتشار عبر المودم عن طريق خطوط الهاتف، التي تقدمها الخدمات الشبكية القديمة مثل كومبوسيرف وبروديجي وإيثرلينك وإي.أو.إل. وبات بإمكان الفيروسات وأحصنة طروادة الحديثة مثل ميليشا (1999) وفيروس الحب (2000) والشيفرة الحمراء (2001) وسلامر (2003) وساسر (2004)،

إصابة حواسب ويندوز في أنحاء العالم بسهولة، مدمرة الأبحاث والوصفات الطبية ورسائل الحب والجداول الإلكترونية التجارية التي نخزنها على الأقراص الصلبة. بين ليلة وضحاها، بتنا جميعاً جزءاً من اللعبة.

تأتي برمجيات الحاسب الخبيثة اليوم في الكثير من الأشكال، لكنها جميعاً تسعى إلى التخريب أو الإزعاج أو السرقة أو إلى تنفيذ فعل غير قانوني أو غير مسموح به على نظام بيانات أو في شبكة:

- تتكاثر فيروسات الحاسب بإقحام نسخة منها في برنامج آخر، تماماً كما يصيب فيروس حقيقي مضيفاً بيولوجياً متاحاً له.
- تسبب الديدان الحاسوبية بدورها الأذى، لكنها تقوم بذلك كبرمجيات مستقلة ولا تتطلب برنامجاً مضيفاً لكي تتكاثر.
- أما أحصنة طروادة، التي سميت كذلك تيمناً بالحصان الخشبي الأسطوري الذي استخدمه الإغريق للتسلل إلى طروادة، فغالباً ما تتنكر كبرمجيات شرعية وتتفعّل باستدراج المستخدم إلى تحميل وتنفيذ الملفات على النظام المستهدف. وغالباً ما تفتح أحصنة طروادة "باباً خلفياً" يمنح المهاجمين تحكماً دائماً بالنظام المصاب. ولا تتكاثر أحصنة طروادة بإصابة ملفات أخرى بمعنى الكلمة، بل تنتشر بإقناع المستخدمين بالنقر على ملف أو فتح ملف مصاب مرفق برسالة بريد إلكتروني.

يدرك كاتبو الفيروسات اليوم أن العامة بدأت تفهم ببطء (ببطء شديد) فحوى الدعوى إلى عدم فتح الملفات المرسلة من غرباء. لذا قام المجرمون بتحديث تكتيكاتهم عبر استخدام ما يدعى التحميل "أثناء التجاوز"، مستخدمين برمجيات خبيثة تستغل ثغرات في لغات الحاسب الخطاطية، مثل جافا وأكتيف إكس، وهي لغات شائعة الاستخدام في متصفحات الويب. لقد انتقل العالم إلى الشبكات، وبات اختراق متصفحات مثل إنترنت

إكسبلورر وفيرفوكس وسفاري معقولاً بالنسبة للمجرمين، وإن كانت طريقة عملهم الجديدة باهظة الكلفة بالنسبة للمستخدمين غير المرتابين. وقد اكتشف الباحثون في بالو ألتو للشبكات أن ما يصل إلى 90 بالمئة من البرمجيات الخبيثة الحديثة تنتشر اليوم بفضل مواقع إنترنت شعبية، تم اختراقها من قبل وصارت تسبب إصابة الحواسب ما إن يمر بها زائر غير مرتاب. وثمة الكثير من الشركات الكبرى، مثل ياهو! البوابة التي يقصدها كثيرون من أنحاء العالم، تعرضت لاختراق مجرمين وراحت بعدها، من دون أن تدري، تسمم زبائنها بالذات الذين كانوا يمرون بها للاطلاع على النتائج الرياضية أو عوائد البورصات.

انفجار البرمجيات الخبيثة

لم يعد هدف القراصنة اليوم هو التهليل، بل صاروا يسعون إلى المال والمعلومات والسلطة. ففي بداية القرن الحادي والعشرين، ومع توصل المجرمين إلى طرق الانتفاع المالي من برمجياتهم الخبيثة عبر سرقة الهوية وغيرها من التقنيات، باتت أعداد الفيروسات الجديدة تحلّق، حتى أصبحت مذهلة في عام 2015. ففي عام 2010، قدر معهد إي.في – تيست الألماني للأبحاث وجود 49 مليون سلالة من برمجيات الحاسب الخبيثة. وفي عام 2011، أفادت شركة ماكافي لمضادّات الفيروسات بأنها تتعرف على مليوني برمجية خبيثة جديدة كل شهر.

وفي صيف عام 2013، أعلنت شركة الأمن السايبري كاسبرسكي أنها كانت تتعرف على حوالى 200000 عينة خبيثة جديدة وتعزلها كل يوم.

إذا ما تناولنا هذه الإحصاءات بتشدّد، آخذين في الاعتبار أن شركات مضادات الفيروسات قد تكون لها دوافعها للمبالغة في حجم المشكلة التي تم تأسيسها لمكافحتها، فقد نميل إلى خفض هذه الأرقام خفضاً هائلاً، بمقدار 50 أو حتى 75 بالمئة. لكن حتى عند ذلك، سيبقى لدينا خمسون

ألف فيروس جديد يتم خلقها كل يوم. فماذا عن جميع تلك الجهود التي تبذل في مجال الأبحاث والتطوير، التي يتطلبها إنشاء كل هذا الحجم من البرمجيات الخبيثة المبرمجة برمجة فريداً على مستوى العالم؟

كما يعلم أيّ رجل أعمال، فإن تكاليف البحث والتطوير كبيرة. لذا فإن العوائد على الاستثمار التي يجب تحقيقها لدعم جهود البرمجة الحاسوبية غير الشرعية، التي يتطلبها الحفاظ على استمرارية الجريمة الدولية المنظمة يجب أن تكون هائلة. وقد ظهرت دراسة موثوقة لجمعية المستهلكين، التي تنشر مجلة كونسيومر ريبورتس (تقارير المستهلكين)، لتؤكد الأثر المتعاظم للبرمجيات الحاسوبية الخبيثة. فقد كشف استطلاع لقرائها أن ثلث الأسر في الولايات المتحدة قد سبق لها أن تعرضت لإصابة ببرمجيات خبيثة خلال العام المنصرم، موقعة تكاليف هائلة تبلغ 2.3 مليار دولار سنوياً. وهؤلاء هم من أدركوا تعرضهم لهجوم فقط.

وهم الأمان

لا يتردد المستهلكون ولا الشركات عن وضع ثقتهم في صناعة برمجيات أمن الحاسب، موكلين إليها مهمة حمايتهم من أية تهديدات يمثلها ظهور برمجيات حاسوبية خبيثة. فوفقاً لدراسة أجرتها مجموعة غارتنر، وصل إجمالي حجم الإنفاق السنوي على البرمجيات الأمنية إلى حوالى العشرين مليار دولار عام 2012. ويتوقع أن يحلّق أكثر بعد ليصل إلى 94 مليار دولار تنفق على الأمن السايبري عام 2017.

إذا ما سألت عما يجدر القيام به حيال الفيروسات الحاسوبية، فسيكون الجواب الأول لمعظم الناس هو استخدام مضادّ فيروسات من شركة ما، مثل سيمانتيك أو ماكافي أو تريند ميكرو. وهو جواب غريزي من جمهور جرى تدريبه جيداً. ومع أن مثل هذه الأدوات ربما أثبتت فائدتها في الماضي، فإنها لا تنفك تفقد فعاليتها فقداناً سريعاً وهو ما تكشفه الإحصاءات على نحو

جليّ. ففي شهر كانون الأول من عام 2012، قرر باحثون من شركة إمبيرفا لدراسات أمن البيانات في ريدوود شورز بكاليفورنيا بالتعاون مع طلاب من جامعة معهد تيكنيون - إسرائيل للتقانة، وضع أدوات مكافحة الفيروسات الشائعة قيد الاختبار. فقاموا بجمع 82 فيروساً حاسوبياً جديداً، ومرّروا هذه البرمجيات الخبيثة على محركات لكشف التهديدات الأمنية تعود إلى أكثر من أربعين من كبريات شركات مكافحة الفيروسات في العالم، كان من بينها مايكروسوفت وسيمانتيك وماكافي وكاسبرسكاي. وخرجت التجربة بمعدل كشف أولي لم يتجاوز الخمسة بالمئة، أي إن 95 بالمئة من البرمجيات الخبيثة قد مرت من دون أن يتم اكتشافها بتاتاً، الأمر الذي يعني أيضاً أن برمجيات مكافحة الفيروسات التي تستخدمها على حاسبك بالذات لا تستطيع أن تكتشف أكثر من خمسة بالمئة من التهديدات الجديدة التي تستهدف جهازك. لو كان لجهاز المناعة في جسمك معدل دفاع مشابه للفظت أنفاسك في غضون ساعات.

بعد ذلك بأشهر، قام كبار مصنعي البرمجيات الأمنية أخيراً بتحديث برمجياتهم، لكن مثل هذا الإجراء غالباً ما يكون غير مجدٍ. فواقع الأمر هو أن المجرمين ومبرمجي الفيروسات يتجاوزون في إبداعاتهم ومناوراتهم بأشواط طويلة صناعة مكافحة الفيروسات، التي أقيمت لتحمينا من التهديدات. والأسوأ من ذلك بعد، هو أن "متوسط وقت الاكتشاف"، أي المدة الزمنية المنقضية بين ظهور برمجية خبيثة "في الغاب" وبين اكتشاف أمرها، في تنامٍ مستمر. فعلى سبيل المثال، اكتشف باحثو مختبر كاسبرسكي في موسكو عام 2012 برمجية خبيثة في غاية التعقيد تعرف باسم فليم، أو الشعلة، كانت تعمل على سرقة البيانات من أنظمة المعلومات في أنحاء العالم على مدى أكثر من خمس سنوات قبل أن يتم اكتشافها. بل إن ميكو هايبونين، مسؤول الأبحاث المرموق في شركة أمن الحواسب إف - سيكيور،

اعتبر فيروس فليم إخفاقاً لحق بصناعة مكافحة الفيروسات، ونوّه إلى أنه وزملاءه ربما كانوا "يغردون خارج السرب" في مجال عملهم بالذات. فعلى الرغم من اعتماد الملايين على هذه الأدوات، بات من الجلي إلى حدٍ ما أن حقبة مكافحة الفيروسات قد ولّت.

من الأسباب التي تجعل من الصعب مواجهة هذا التنوع في التهديدات التقانية في حياتنا اليوم، هو التنامي المستمر في عدد ما يدعى هجومات اليوم صفر. وهجوم اليوم صفر هو هجوم يستغل نقطة ضعف لم تكن معروفة من قبل في تطبيق حاسوبي، ولم يتسنّ للمطورين ولكوادر الأمن الحاسوبي إصلاحها. لكن بدلاً من أن تبحث شركات البرمجيات الأمنية بنفسها عن نقاط ضعف كهذه، لا تأخذ هذه الشركات في اعتبارها سوى النقاط المعروفة. وهي تقوم بالحجر على سلسلة من التعليمات إذا ما تطابقت مع سلسلة تعليمات أخرى تم التعرف عليها مسبقاً. فالأمر أشبه بنشر ملصق يطالب بالتبليغ عن بوني وكلايد لأننا نعلم أنهما قد قاما بالسطو على بنوك من قبل، حيث سيعرف محاسبو المصارف كيف يبقون متيقظين في انتظار الثنائي المطلوب، لكن ما دام لم يظهر أحد تنطبق عليه الأوصاف، فإن المحاسبين سيتراخون في المراقبة إلى أن تحدث عملية سطو جديدة على بنك، هذا كل ما في الأمر. لا تنفكّ هجومات اليوم صفر تزداد ظهوراً مستهدفة طيفاً واسعاً من المنتجات التقانية الشائع استخدامها في حياتنا اليومية ومصيبة كل شيء، من نظام ويندوز من مايكروسوفت إلى موجهات لينكسيس الشبكية وقارئ البي.دي.إف ومشغل الفلاش من أدوبي واسع الانتشار.

تعلّم القراصنة مع الوقت أنهم كلما أثاروا ضجيجاً أثناء اختراقهم نظامك، سارعت إلى حل المشكلة وطردهم خارجاً. فصار همّهم هو السرية والتخفي، كما لو كانت لديك خلية نائمة على حاسبك. وقد يتهيأ لك أن

معدل اكتشاف فيروسات الحاسب الذي لم يتجاوز الخمسة بالمئة وفقاً لما كشفته دراسة إمبيرفا لا ينطبق سوى على المواطنين العاديين، الذين يستخدمون برمجيات أمنية شخصية في منازلهم، وأن الشركات، بما لديها من ميزانيات هائلة تخصصها لتقانة وأمن المعلومات، سيكون حظها أوفر، لكن هذا ليس دقيقاً. فعشرات الآلاف من الهجمات الناجحة التي استهدفت شركات ومنظمات مستقلة وحكومات كبرى في أنحاء العالم تثبت أن الشركات، على الرغم من كل ما تنفقه لهذا الغرض، لا توفر حماية أكبر بكثير لمعلوماتها.

وفقاً لتقرير فيريزون حول التحقيقات في انتهاكات البيانات لعام 2013، أثبتت معظم الشركات أنها ببساطة غير قادرة على اكتشاف اختراق مهاجم لنظمها المعلوماتية. ويشير المسح الهامّ الذي نفذته فيريزون للخدمات التجارية بالتعاون مع دائرة الاستخبارات الأميركية والشرطة الوطنية الهولندية والوحدة المركزية للجريمة الإلكترونية في شرطة المملكة المتحدة، إلى أن ما معدله 63 بالمئة من الانتهاكات التي استهدفت شركات تجارية قد استغرقت ما لا يقل عن شهرين حتى تم اكتشافها. وتدقّ دراسة مشابهة لمؤسسة ترست ويف هولدينغس ناقوس الخطر، إذ كشفت أن الزمن الوسطي الذي يفصل بين الاقتحام الأولي لشبكة شركة ما وبين اكتشاف الهجوم كان يبلغ 210 أيام، أي حوالى سبعة أشهر تُمنح للمهاجم، سواءٌ كان من عالم الجريمة المنظمة أو أحد المنافسين أو حكومة أجنبية، يمكنه خلالها أن يتجول في شبكة المؤسسة خلسة دون قيود، يسرق الأسرار ويجمع معلومات تنافسية ويخترق الأنظمة المالية ويختلس معلومات تعريف شخصية للزبائن، مثل أرقام بطاقاتهم الائتمانية.

وحين تكتشف شركة في النهاية وجود جاسوس رقمي في صفوفها وتعرض نظام المعلومات الحيوي لديها للاختراق، فإن مكتشف الانتهاك، في 92

بالمئة من الحالات، لا يكون مسؤول المعلومات في الشركة ولا الفريق الأمني ولا مدير النظام. بل يتم إبلاغ الضحية من قبل القوى التنفيذية أو من زبون ساخط أو من متعاقد. وإذا كانت كبرى الشركات في العالم التي تنفق مجتمعة الملايين على الدفاع السايبري ولديها أقسام من المختصين الذين يعملون على مدار الساعة لحماية شبكاتها، سهلة الاختراق من قبل المهاجمين إلى هذا الحد، فإنّ الإمكانات المتاحة أمام المستخدمين المنزليين لحماية معلوماتهم تبدو ضئيلة بالفعل.

ما مدى صعوبة اختراق نظام حاسوبي اعتيادي اليوم؟ الأمر سهل إلى حد مضحك. فوفقاً لدراسة أعدها مركز فيريزون، فإن القراصنة، إذا ما وضعوا شبكتك نصب أعينهم، يتمكنون من اختراقها في 75 بالمئة من الحالات خلال بضع دقائق. كما نوهت الدراسة عينها إلى أن هذه المدة ترتفع إلى بضع ساعات في 15 بالمئة من الحالات فقط. إنها نتائج ذات تبعات كبرى. فابتداءً من اللحظة التي يقرر فيها المهاجم أن يستهدف عالمك، ستكون اللعبة قد انتهت خلال بضع دقائق في 75 بالمئة من الحالات. سيوسعونك ضرباً ويطرحونك أرضاً قبل أن تدري ما الذي ارتطم بك. في عالم اليوم، يعيش القراصنة أحراراً بلا قيود داخل نظم بياناتك الخاصة لشهور طويلة، يراقبون وينتظرون ويترصدون، فينهبون كل شيء، من كلمات المرور إلى مشاريع العمل والصور الذاتية القديمة. فما أنت سوى دريئة سهلة وصيد يسير. فكم غريب أمرنا حين نتهاون في هذا الخصوص كمجتمع، فلو شاهد أحدنا لصاً في منزله يراقب ما يفعل في الحمام لطلب الرقم 911 (أو ربما صرخ عوضاً عن ذلك، أو بحث عن سلاح). أما في الفضاء السايبري، فإن ذلك يحدث يومياً، إلا أننا نلزم الصمت هناك، بل إننا ننعم بجهلنا لحقيقة التهديد القائم على الرغم من نقاط الضعف التي لدينا ورغم الأشرار الذين يحومون حول رؤوسنا أثناء نومنا.

لا تنفك ترتفع تكاليف انعدام الأمن السايبري الشامل الذي نعانيه. ومع أن الشركات في أنحاء العالم ربما ستنفق حوالى مئة مليار دولار عام 2017 على مختلف الاستعدادات الأمنية، سواءُ على شكل برمجيات أم على شكل تجهيزات، فإن هذا الثمن ما هو سوى البداية إذا ما فكرنا بالأثر الاقتصادي الكامل لهشاشتنا التقانية. ولنأخذ على سبيل المثال الهجوم السايبري الذي استهدف عام 2007 شركة تي.جي.إكس، شريكة سلسلة تي.جي. ماكس ومارشالز في الولايات المتحدة وتي.كي. ماكس في أنحاء أوروبا.

في تلك الحادثة، قام المهاجمون بسرقة تفاصيل البطاقات الائتمانية لأكثر من خمسة وأربعين مليون زبون، ما يجعلها أكبر حالة اختراق لمحل تجزئة على الإطلاق آنذاك، بل إن مراجعات المحكمة في ما بعد بينت أن العدد الحقيقي للضحايا من الزبائن يقارب الأربعة والتسعين مليوناً. ومع أن تي.جي.إكس قد توصلت إلى تسوية مع فيزا وماستركارد وزبائنها بقيمة 256 مليون دولار، فإن كثيراً من المحللين يعتقدون أن التكاليف الحقيقية يمكن أن تصل بسهولة إلى المليار دولار. فمعهد بونيمون الذي يجري أبحاثاً مستقلة على سياسات حماية البيانات وأمن المعلومات، والذي يعتبر من أكثر مصادر الأبحاث موثوقية في مجال التكاليف المترتبة على اختراقات البيانات، ينوّه في سياق حساب تكاليف الاختراقات الأمنية السايبرية إلى أهمية أن يتجاوز تحليل الخسائر كثيراً المبالغ المختلسة مباشرة من الزبون.

فعلى سبيل المثال، يترتب على الشركة الضحية المستهدفة بالهجمات، كشركة تي.جي.إكس، أن تنفق مبالغ مناسبة على اكتشاف الاختراق واحتواء المهاجمين والتحقيق في القضية وتحديد هوية المذنبين، كما على إصلاح شبكة الحواسب لديها وإعادتها إلى العمل. علاوة على ذلك، كثيراً ما تعاني المبيعات انحسارات كبيرة مع تجنب الجمهور اليقظ لخدمات الشركة، التي باتت تعطي انطباعاً بأنها غير آمنة. ناهيك برسوم استبدال البطاقات

الائتمانية (التي تقدر حالياً بـ 5.10 دولارات للبطاقة الواحدة)، وخدمات مراقبة رصيد المستهلك التي سيترتب على الشركة الضحية شراؤها لمنع استهداف زبائنها بعمليات احتيال بالبطاقات الائتمانية، وارتفاع رسوم التأمين ضد الهجمات السايبرية. ليس صعباً إذاً إدراك كيف يمكن لقيمة هذه الخسائر أن تتصاعد، ولا عجب في أن نجد معظم الشركات لا تعترف إلا على مضض بتعرضها للاختراق، بل إن كثيراً منها ينكر الهجوم لأطول وقت ممكن.

بل ثمة بعد المزيد من التكاليف التي لا بد من أخذها بالاعتبار، مثل العقوبة التي تتعرض لها الشركات الضحية في سوق الأسهم على شكل تراجعات في أسعار أسهمها بعد تعرضها لانتهاك سايبري. وقد حدث ذات مرة أن شهدت شركة غلوبال بيمينتس قيمتها السوقية تنسلخ بنسبة 9 بالمئة في يوم واحد، إلى أن أوقفت بورصة نيويورك التعامل بحصصها. ومما يزيد الطين بلة من الناحية المالية في مثل هذه الحالات، الدعاوى القضائية التي يرفعها زبائن الشركة ومالكو أسهمها ومراقبوها. ويخلص معهد بونيمون إلى أن الشركات مهددة بتكاليف تصل إلى 188 دولاراً مقابل كل سطر بيانات تتم سرقته. فإذا ضربنا هذا المبلغ بمئة مليون هو العدد التقريبي للسجلات التي سرقت من شركة تي.جي.إكس، صار من السهل أن ندرك سرعة تصاعد تكاليف مثل هذه الاختراقات ونموها الأسّي.

خلاصة القول إننا كمجتمع، ما بين المبالغ المنفقة على الإجراءات الوقائية غير الفعالة في معظمها، ثم على إغلاق الثغرات السايبرية بعد أن نُخرج أحصنة طروادة من حدودنا (ونبقي على المهاجمين في الداخل)، ندفع ثمناً باهظاً نتيجة انعدام الأمن التقاني. والأسوأ من ذلك بعد، هو أن تنامي اتصالنا بالعالم الشبكي وما يعني ذلك من اعتمادنا الجذري على تقانات قابلة للاختراق بمجملها، قد يؤذينا بطريقة أكثر إيلاماً من مجرد إفراغ

جيوبنا جميعاً.

لقد فقدت الإنترنت براءتها، فعالمنا المتشابك لا ينفك يزداد خطراً وكلما أدخلنا تقانات معرضة للاختراق في حياتنا، ازداد ضعفنا. والثورة الصناعية القادمة، أي ثورة المعلومات، جارية على قدم وساق، وسيكون لها آثار كبرى غير ملحوظة على أمننا الشخصي والعالمي. لكن مهما بدت قاهرة التهديدات التي تحوق اليوم بالأفراد والمنظمات، بل وحتى بالبنى التحتية الحساسة، ثمة أيضاً قطار تقاني يغادر المحطة توًّا منطلقاً بسرعة ليواكب هذه التطورات بتسارع أسّي، وله دلالات في كل مكان إذا عرف المرء أين ينظر.

ثمة تقانات ناشئة حديثاً تلوح في الأفق، مثل الروبوتيات والذكاء الصنعي وعلم الجينات والبيولوجيا التركيبية وتقانة النانو والتصنيع الثلاثيّ الأبعاد وعلم الدماغ والواقع الافتراضي، سيكون لها أثر هائل على عالمنا، فهي تفرض طيفاً من التهديدات الأمنية سيجعل الجريمة السايبرية الشائعة اليوم تبدو أشبه بلعبة أطفال. ولن يستغرق الأمر سوى بضع سنوات فقط حتى يصبح لهذه الابتكارات الجديدة دور أساسي في حياتنا اليومية، إلا أنه ما من دراسة معمقة ومتوسعة قد استُكملت لتساعدنا على فهم المخاطر الجانبية غير المتوقعة التي تفرضها.

لقد بقي عمق هذا التحول ومداه والمخاطر الملازمة له غير ملحوظين في معظمهما. لكن قبل أن ندرك الأمر، سيكون مجتمعنا قد وصّل ما ينوف على تريليون جهاز جديد بالإنترنت، وهي كلها أجهزة ستنفذ إلى جميع جوانب حياتنا. وستقوم هذه الاتصالات الدائمة بربطنا ببشر وآلات، خيرهم وشرّهم، في مختلف أنحاء المعمورة، وستكون متشابكة في عالم كامل من الوعي الجمعي ينمو نمواً أسّياً. والنتيجة ستكون أن التقانة لن تعود مسألة متعلقة بالآلات وحسب، بل ستصبح سيرة للحياة قائمة بذاتها. أما أولئك

الذين يعلمون كيف تعمل هذه التقانات الكامنة، فستكون لديهم قدرة أكبر على تسخيرها لمنفعتهم، كما رأينا سابقاً، ليبقى الإنسان العادي هو المتضرر. ومن الوارد جداً لهذه الوفرة التقانية التي نقبلها في حياتنا دون التفكير أو التدقيق فيها كثيراً، أن تعود وتلدغنا. إنها مخاطر تنذر بالعالم الجديد، ذلك المستقبل الذي لم نستعدّ لاستقباله على الإطلاق. يتناول هذا الكتاب علاقة الإنسان بالآلة وكيف يمكن للعبد أن يصبح هو السيد.

الفصل الثاني
انهيار النظام

إذا استمررنا في تطوير التكنولوجيا دون حكمةٍ أو تعقّل، فقد يثبت خدمنا أنهم جلادونا.

عمر ن. برادلي

لا بد أن هناك خطأً ما في الإشارات. كان ذلك يوم ثلاثاء في أوائل شهر كانون الأول عام 2008 في مدينة لودز في بولندا، عندما انحرفت عربة ترام نحو اليسار. لم يكن ذلك بحد ذاته أمراً غريباً، لولا حقيقة أن السائق كان يحاول الانعطاف بالقطار إلى اليمين. وما كانت سوى لحظات حتى انزلقت السيارات الخلفية على السكة الحديدية، لتصطدم بقطار آخر وتنتهي إلى توقف صاخب.

كان من المذهل، نظراً لحجم الاصطدام، أنه لم يُقْتَلْ أحد، لكن العديد من الركاب أصيبوا بجروح، بينما بقي آخرون يحكّون رؤوسهم حيرة. فما الذي جرى؟ بدلاً من التكهن بمجرد عطل في الدارة أو بخطأ بشري ارتكبه السائق، شكّ مهندسو السكك الحديدية بلعبة قذرة. وكانوا محقين في ذلك، ولكن لأسباب عديدة كانوا على الأرجح يجهلونها.

وسرعان ما تكشّف أن صبياً بارعاً في الحواسيب يبلغ عمره أربعة عشر عاماً، قد اخترع جهاز إرسال عن بعد، يعمل بالأشعة ما تحت الحمراء قادراً على التحكم بكافة الوصلات الموجودة على خط النقل. وكان الصبي قد أمضى عدة أشهر في دراسة نظام السكك الحديدية للمدينة، ليحدد النقاط الأفضل لإعادة توجيه القطارات بما سبب أكبر قدر من الفوضى، ثم اخترق مفاتيح التحويل في أنحاء المدينة ليعيد توجيه القطارات بأمر منه.

بعبارة أخرى، كان الصبي قادراً على استخدام نظام قطارات المدينة "كمجموعة ألعاب شخصية"، من خلال اختراق بنية النقل التحتية في

المدينة والتحكم بها إلكترونياً. وكان يُعتقد أن الطفل قد استخدم الجهاز في مناسبات عديدة، فقد اعترف عندما تم كشفه واعتقاله بأنه فعل فعلته، مثل القرصان الذي هاجم مات هونان، لمجرد التسلية.

لكن هذه التسلية أدت إلى انحراف أربعة قطارات عن مسارها، وكان لها بسهولة أن تسبب وفاة عدد من الركاب. أثار هذا الحادث الاستثنائي غضب العديد من محللي الأمن، لأنه لم يُبْذل الكثير للحفاظ على سلامة البنية التحتية الهامة في المدينة. وكانوا على حق في خشيتهم من أنه إذا كان بمقدور فتىً في الرابعة عشرة من عمره أن يعبث بمفرده بشبكة نظام للنقل، مخلفاً وراءه فوضى كهذه لمجرد تسليته الشخصية، فما الذي سيردع المجرمين والإرهابيين والدول المعادية من القيام بالعمل نفسه؟

شبكة المعلومات العالمية الهشّة

سبق أن رأينا كم من السهل اختراق أغلبية أنظمة الحواسب، وكم هو سريع تنفيذ مثل هذا العمل. وقد أثبتت تجربة مات هونان أن حياتنا الرقمية معرضة لأن يمحى أثرها في لحظة. كان على كل من ت.ج.ماكس وسيتيبانك، أن يتعلما درساً قاسياً عما يمكن أن يحدث عندما يضعك مجرمون بعيدون عنك آلاف الأميال نصب أعينهم. والمخاطر المذكورة تبين لنا، أنه لا بأس ببعض الحذر قبل إضافة أي شيء يمكن وصله بالكهرباء أو له بطارية إلى شبكة المعلومات العالمية، لكننا مع ذلك نندفع بكامل قوتنا في حبنا المتزايد للأشياء المرتبطة بالتكنولوجيا.

نتيجةً لذلك، تتكاثر اتصالاتنا بأنظمة حاسوبية بطرقٍ لا نفهمها. وهذه الاتصالات غير موثوقة وقابلة للاختراق، فهي أساس هشّ لا تُبنى عليه معلومات المجتمع في القرن الحادي والعشرين. لكن هذا هو ما نقوم به عملياً. ليست حواسبنا الشخصية وحواسبنا في العمل هي الوحيدة المتصلة بالإنترنت، بل أيضاً جميع البُنى التحتية الحساسة التي يعتمد عليها

مجتمعنا الحديث، كشبكة الكهرباء وأنابيب الغاز وأنظمة تحويل911 وأنظمة التحكم بالملاحة الجوية، والبورصة ومياه الشرب وإنارة الشوارع والمستشفيات والمرافق الصحية. بل إن الصحة العامة لدينا تعتمد برمتها على التكنولوجيا والإنترنت في عملها. في هذا العالم الجديد الرائع، أخرجنا الإنسان من اللعبة ووضعنا العمود الفقري للحضارة في عهدة الآلات.

جميع معاملات بطاقات الائتمان وطرفيات نقاط البيع، والصرافات الآلية التي تحافظ على تدفق الاقتصاد ونشاط الرأسمالية، سوف تنتهي إلى توقف صارخ إذا كفت الحواسيب عن تشغيل الشبكة. فالحواسب هي التي تحدد كيفية ومكان وزمان توجيه الكهرباء لضمان استقرار شبكة الطاقة. بينما تقوم أنظمة التحويل المدعومة بالحواسب بالحفاظ على مسار سيارات الشرطة وسيارات الإسعاف وسيارات الإطفاء، ممكّنة مسؤولي العمليات من معرفة العناصر المتوفرة وأقرب من يمكنه الاستجابة في حالة الطوارئ. لتكوين فكرة خاطفة عما سيؤول إليه حال هذا العالم البائس من دون الحواسيب والكهرباء، ليس على المرء سوى أن يشغل التلفاز ليعاين بنفسه نهاية العالم الذي ستُجهز عليه التقانة، كما يتبين في عروض مثل "الميت الذي يمشي" أو في أفلام مثل "كوكب القردة" و"موت قاس". وبعيداً من الخدع السينمائية في هوليوود، تبقى البنى التحتية الهامّة المعتمدة على الحواسب معرضة وبشكلٍ متزايد للهجمات، وهي ستهتز بعمق إذا ما حدث خطأ في أنظمتها، الأمر الذي قد يكون أثره كارثياً بكل معنى الكلمة.

تستخدم الكثير من البنى التحتية الهامة في العالم أنظمة رقابية للتحكم وجمع البيانات (سكادا) في عملها. وهي أنظمة تقوم "تلقائياً" بمراقبة وتنظيم عمليات التحويل والتصنيع وغيرها من فعاليات التحكم بالعمليات، معتمدة في ذلك على حساسات تقوم بجمع البيانات الرقمية الراجعة. وهذه الأنظمة هي عبارة عن أنظمة حاسوبية متخصصة، غالباً ما

تكون قديمة، تتحكم بالقطع المادية للأجهزة التي تقوم بكل شيءٍ، بدءاً من توجيه القطارات على سككها وصولاً إلى توزيع الطاقة عبر كافة أرجاء المدينة. ويجري العمل على نحو متزايد على وصل أنظمة سكادا هذه بشبكة إنترنت أكثر اتساعاً، الأمر الذي يفرض تبعات كبيرة على أمننا العام. لكن لسوء الحظ، لم يأخذ تصميم هذه الأنظمة في اعتباره مسألة الأمن، ولم تتم هندسة هذه الأنظمة بحيث تتحلى بالمقاومة في عالم متصل بالإنترنت. والمشكلة أسوأ مما تتصور: ففي شهر تموز من عام 2014، أجريت دراسة حول شركات البنى التحتية الحساسة تناولت قطاعات متنوعة، وكانت النتيجة أن 70 بالمئة منها تقريباً يعاني ثغرة أمنية واحدة على الأقل، كانت قد أدت خلال الأشهر الاثني عشر المنصرمة إلى خسارة معلومات سرّية أو إلى عرقلة فعلية للعمليات.

فما الذي يمكن لقرصان فعله إذا وصل إلى هذه الأنظمة؟ لنأخذ على سبيل المثال الأنظمة المعلوماتية المعقدة، التي تنظم محطة معالجة المياه المحلية. يقوم نظام سكادا باستمرار بقياس وتنظيم الخليط المناسب من الموادّ الكيميائية لتنقية مياهنا وجعلها صالحة للشرب. ولكن ماذا لو تم اختراق هذا النظام؟ هل يمكن لمقدار خاطئ من الموادّ الكيميائية الممزوجة أن يلوث مياهنا بدلاً من تنقيتها؟ قد يبدو ذلك مضحكاً، ولكن تقريراً نشرته إذاعة بي.بي.سي عام 2011، يفيد بالفعل بقيام قراصنةٍ بشنّ هجوم على قسم المياه والصرف الصحي في جنوب هوستون في ولاية تكساس. وبعد تعقب عنوان المهاجم على الإنترنت تبين أنه روسي. وكان القراصنة، وفقاً لما قيل، قد قاموا بتشغيل وإيقاف إحدى المضخات بشكلٍ متكرر وبسرعة مما أدى إلى تعطلها. ومع أن أحداً لم يمرض خلال الهجوم، فإنه يثبت فرضيتنا.

أيّ اختراقات يمكن أن تتعرض لها البنية التحتية بعد؟ ما من حدٍّ سوى السماء، كما اكتشف برج المراقبة التابع لإدارة الملاحة الجوية الفدرالية في

وورسيستر، ماساتشوستس عام 1998. فقد استخدم مراهق من أبناء المنطقة معرفته الحاسوبية ليقطع الاتصالات بين الطائرات القادمة والبرج، بل إنه أطفأ إنارة مدرج الهبوط حاجباً إياه عن الطائرات القادمة. ومع أن أحداً لم يُقتل جراء الحادثة، فإن إمكانية حدوث كارثة كان واضحاً. وثمة بالطبع العديد من الهجمات الأخرى التي استهدفت بنىً تحتية معلوماتية حساسة وهامة في أنحاء العالم. ولعل أقدم هذه الهجمات كانت في مقاطعة ماروشي، كوينزلاند في أستراليا عام 2001 حين هاجم قرصانٌ محطة لمعالجة مخلفات الصرف الصحي وتمكّن من السيطرة على أنظمة التحكم الصناعية، "مسبباً تدفق ملايين الليترات من المخلفات الخامة إلى المتنزهات العامة والأنهار المحلية، وحتى إلى أرض فندق هيات ريجينسي". ودمّر الهجوم كميات لا بأس بها من الحياة البحرية والنباتية، ناهيك بالتهديد البيئي للسكان المحليين.

لعل أكثر الأنظمة حساسية وعرضة للهجوم هي شبكة الكهرباء الوطنية. فمن دون الكهرباء ستتوقف كافة المعامل عن العمل، ولن يكون هناك بالتالي إنارة ولا مصاعد ولا صرافات آلية ولا إشارات مرور ولا قطارات أنفاق، ولا أبواب آلية للمرائب ولا ثلاجات ولا وقود. وعندما تتوقف البطاريات الاحتياطية ومولدات الطوارئ عن العمل، الأمر الذي لا محيد عنه في نهاية المطاف، لن تبقى هناك اتصالات خلوية ولا إنترنت. وعلى الرغم من اعتمادنا الحيوي على الكهرباء كبنيةٍ تحتية تكنولوجية هي الأكثر مركزية في حياتنا المعاصرة، فإن وزير الدفاع الأميركي السابق ليون بانيتا أوضح أن "حادثة بيرل هاربر المقبلة التي سنواجهها قد تكون هجوماً سايبرياً يشلّ" أنظمة الطاقة وشبكة الكهرباء لدينا.

وجدت مخاوف بانيتا ما يبررها إلى حد كبير في تقرير لقسم الطاقة الأميركية، أشار إلى أن شبكة الطاقة الأميركية، التي غالباً ما تُوصف بالآلة

الأكثر تعقيداً في العالم، تقوم بربط مئة وخمس وثمانين محطة طاقة مستقلة ولديها أكثر من 450,000 ميل من خطوط نقل التوتر العالي. إلا أن سبعين بالمئة من العناصر الأساسية المكونة للشبكة يزيد عمرها عن خمس وعشرين سنة. ويستخدم كل عنصر من هذه العناصر أنظمة سكادا أقدم بكثير تسهُل مهاجمتها وتتعرض لهجمات مستمرة.

كشف تحقيق قامت بها لجنة الطاقة والتجارة المنزلية عن أن أكثر من اثنتي عشرة شركة مرافق أميركية، قد سجلت هجمات سايبرية "يومية" أو "مستمرة" أو "متكررة" تراوحت بين التصيد والعدوى بالبرمجيات الخبيثة، بل وحتى أخذ العينات لأغراض عدوانية. بل إن إحدى هذه المرافق كانت هدفاً لأكثر من 10,000 محاولة هجوم سايبري في كل شهر. وختم التقرير بالإشارة إلى أن الحكومات الأجنبية والمجرمين والقراصنة العشوائيين كانوا جميعاً يعملون بدأب، تخطيطاً أو تنفيذاً، لتدمير الشبكة. وتؤكد النتائج المبنية على بيانات سابقة صادرة عن مسؤولي استخبارات، ومنشورة في صحيفة وول ستريت جورنال أن جواسيس سايبريين قد "اخترقوا الشبكة الكهربائية الأميركية مخلفين وراءهم برامج يمكن استغلالها لتعطيل النظام". وتابع المسؤولون أنفسهم حديثهم، مشيرين إلى أن جواسيس من روسيا والصين يقال إنهم قاموا برسم خريطة للشبكة الأميركية، بحيث يتمكنون في أوقات الأزمات والحروب مع الولايات المتحدة الأميركية من تعطيل الشبكة الكهربائية الأميركية برمتها.

يخطط الإرهابيون بدورهم لشن هجمات رقمية على البنية التحتية الأميركية. ففي صيف عام 2012 كشف مكتب التحقيقات الفدرالي عن شريط فيديو صادر عن قسم الإعلام في تنظيم القاعدة المسمى "السحاب"، تدعو فيه المنظمة الإرهابية "مجاهديها المتخفين" للقيام بموجات من الهجمات الإلكترونية ضد الشبكات الأميركية، سواء الحكومية منها أو تلك

المرتبطة بالبنى التحتية، بما فيها الشبكة الكهربائية. كما كشفت تحقيقات أقدم لمكتب التحقيقات الفدرالي عن العديد من الحالات التي قامت فيها القاعدة بالبحث عبر الإنترنت عن أهدافٍ لها ومراقبتها، كأنظمة هواتف الطوارئ ومحطات توليد الكهرباء ومرافق توزيع المياه ومعامل الطاقة النووية وشبكات تخزين الغاز في الولايات المتحدة.

بل إن المنظمة الإرهابية وضعت خططاً موسعة كاملة لاستهداف البنى التحتية الهامّة التي ستهاجمها عبر جمع صور للأهداف المطلوبة ووضع ملاحظات مفصلة وإجراء عمليات البحث عبر الإنترنت.

يعمل القراصنة أيضاً على استيعاب وكشف واستثمار نقاط ضعف أنظمة سكادا، وغيرها من البنى التحتية الهامّة، التي تعتمد على المعلومات. ففي مؤتمر كاوُس للاتصالات، وهو تجمع سنوي خاص بالقراصنة يُعقد في ألمانيا، يوضح المحللون من خلال عملية البحث العملي كيفية تحقيق سيطرةٍ كاملة على البنى التحتية الصناعية في مجالات الغاز والمواد الكيميائية والبترول والطاقة. لكن ما لا يقل عن ذلك إثارةً للقلق هو قيام القراصنة بمشاركة هذه المعلومات في ما بينهم، بل إنهم قاموا بإنشاء قواعد بيانات شاملة وقابلة للبحث متاحة للعموم تحتوي نقاط ضعف معروفة، يمكن استغلالها للسيطرة على البنى التحتية الهامة. تقدم إحدى هذه القواعد البيانية، وتعرف باسم شودان، تلميحات حول كيفية اختراق أي شيء، بدءاً بمحطات الطاقة ووصولاً إلى توربينات الرياح، ويمكن إجراء البحث فيها وفقاً للبلد أو الشركة أو الجهاز، حيث تقدم دليلاً مساعداً لتذليل العقبات التقنية والمعرفية التي تقف أمام أي شخص غير عارف يرغب في اختراق البنى التحتية لدينا. وقد أصبحت شودان بالنسبة للقراصنة الطامحين لبسط سيطرتهم على عالمنا المترابط، بمثابة محرك البحث غوغل في الواقع، أما إغلاقها فهو أمر شبه مستحيل لأنها موجودة على مخدمات متعددة في

الدول الأجنبية حول العالم كما أن نشر نقاط ضعف لأي نظام لا يعتبر جريمةً في معظم هذه الدول حالياً.

تولي عصابات الجريمة المنظمة اهتمامها للهجمات على البنى التحتية كوسيلةٍ منطقية للابتزاز المالي من المؤسسات والحكومات. ووفقاً للتقارير، فقد وقعت مثل هذه الحوادث في البرازيل بين عامي 2005 و2007، عندما حدثت موجة من الهجمات الإلكترونية في شمال ريو دي جانيرو وفي ولاية إسبيرتو سانتو. في تلك الحادثة، بقي حوالى ثلاثة ملايين شخص في الظلام عندما عجز مزود الكهرباء المحلي عن تلبية متطلبات تحالف للعصابات محلية. نتيجة لذلك، أُجْبِرت مدينة فيتوريا، وهي واحدة من أضخم المدن المنتجة للحديد الخام في العالم، على إيقاف العمل في عدد كبير من مصانعها، ما كلّف الشركة حوالى سبعة ملايين دولار. أكد هذه الهجمات موظفو الاستخبارات الأميركية والباحثون الأمنيّون، بل وحتى الرئيس الأميركي أوباما، وإن بشكلٍ غير مباشر، حينما قال: "نعلم أن المتطفلين الإلكترونيين... في دول أخرى... قاموا بفرض الظلام على مدنٍ بأكملها".

من هو؟

لاحظ الجنرال الصيني المشهور سون تزو، مؤلف كتاب فن الحرب، ببراعةٍ قبل اختراع الإنترنت بمئة وخمس وعشرين سنة، أنه "إذا كنتم تعرفون عدوكم وتعرفون أنفسكم فلن تكونوا عرضة للخطر وإن خضتم مئات المعارك". أي إننا لكي نفهم التهديدات التكنولوجية الواسعة التي تواجهنا، علينا أولاً فهم طبيعة أعدائنا. فلكل عدو وسائله وحوافزه، ولكن القاسم المشترك بينهم جميعاً هو الخطر الذي يفرضه كل منهم على عالمنا الشديد التشابك.

الشخصيات المسؤولة عن الهجمات الإلكترونية متنوعة، فمنها الدول القومية، وعصابات الأزقة، وعصابات الجريمة المنظمة العابرة للحدود،

والأجهزة الاستخبارية الأجنبية، والناشطون - القراصنة، والكوادر العسكرية، والمقاتلون السايبريون، والمقاتلون بالوكالة تحت رعاية دول، والقراصنة المبتدئون، وقراصنة الأماكن العامة، وقراصنة الهواتف وقراصنة بطاقات الائتمان وقراصنة البرمجيات، والعناصر الداخلية الساخطة وجواسيس الصناعة. كلٌّ منهم يؤدي دوره في ما يطلق عليه الجيش الأميركي اسم "الميدان الخامس" للمعركة، أي الفضاء السايبري (بعد عسكرة البر والبحر والجو والفضاء في الأجيال السابقة).

غالباً ما تستخدم هذه المجموعات التكتيكات نفسها، وإن بدرجات مختلفة من التعقيد. لكن جميع المهاجمين يستفيدون من الطبيعة غير المتناسقة للتكنولوجيا، إذ يتوجب على المدافع أن يبني جداراً متماسكاً ليبعد المتطفلين، بينما يحتاج المهاجمون إلى العثور على نقطة ضعف واحدة في هذه الدرع الواقية ليقوموا بهجومهم من خلالها. ويوجد بين هذه الفئات المتنازعة في الحرب السايبرية السرية نوع من التعاون، مُدرك وغير مُدرك في آن معاً، يتعلم فيه اللاعبون من النجاح العملياتي لبعضهم البعض ويحاكونه. فتجري العصابات الإجرامية المنظمة العابرة للحدود، على سبيل المثال، عمليات استطلاع متطورة في التخطيط لهجماتها، ولكنها على الأغلب تعتمد على عصابات الأزقة لتنفيذ تفاصيل خططها، كما يحدث عندما تحتاج إلى وضع أجهزة قشط على الصرافات الآلية أو إلى غسيل الأموال، أو الإحاطة بالبضائع المسروقة على موقع إيباي. وتتعلم المنظمات الإرهابية من مجرمي الإنترنت، فتخترق المواقع للحصول على الأموال اللازمة لتمويل العمليات عبر العالم. وقد تشكل بعض الفرق الوطنية من المواطنين جماعات على الإنترنت، بإشراف متبرعين مدعومين من الدولة في دولٍ مثل الصين وروسيا وإيران، ويتمتعون باستحسانٍ ضمني وتمويلٍ وتدريب، وعندها يشاركون التقنيات والأدوات نفسها مع الحكومات

الراعية لهم. فثمة نوع من التكافل في الأوساط السايبرية السرية وتوافق في المناهج يجمع بين المصادر المختلفة للتهديدات.

لعل النظرة الأولى التي تبدر إلى أذهاننا عندما نفكر بالقرصان، هي تلك الصورة الشائعة لفتى يعيش في سرداب منزله متسمّراً أمام لوحة المفاتيح ومحاطاً بأكياس الشيبس الفارغة وعلب الكولا المبعثرة، محاولاً تغيير علاماته المدرسية من خلال اختراق حواسيب مدرسته (كما فعل ماثيو برودريك في فيلم ألعاب الحروب عام 1983). ففي بدايات عمليات الاختراق عبر الشبكة، كانت أنظمة الهاتف هي الهدف الذي يجذب القراصنة. فكان من أطلق عليهم "مهووسو الهواتف" يتلاعبون بالشبكة ليتجنبوا التكاليف الباهظة المترتبة على المكالمات البعيدة. ولا يجوز هنا نسيان القرصانين اللذين أمضيا جزءاً من شبابهما حتى عام 1971 على اختراع "الصناديق الزرقاء"، وهي أجهزة قادرة على اختراق شبكة الهاتف والقيام بمكالمات مجانية، وكان هذان القرصانان هما ستيف ووزنياك وستيف جوبز. حيث قام الاثنان ببيع هذه الأجهزة لطلاب جامعة كاليفورنيا في بيركلي، كوسيلة لجني الأموال اللازمة لتمويل مشروع آخر قيد الإنشاء وهو شركة أبل للحواسب.

ومع مرور الوقت، ظهر قراصنة بارزون أمثال كيفين ميتنيك وكيفين بولسن. ومن المعروف أن ميتنيك قد تمكن من اختراق حواسب شركة ديجيتال إيكويبمنتس (المعدات الرقمية) عندما كان في السادسة عشرة من عمره، وأنه مضى في سلسلة من الاختراقات جعلته يكسب حنق مكتب التحقيقات الفدرالي وامتيازاً، لكونه "أكثر القراصنة الأميركيين المطلوبين للعدالة". فعملية الاختراق العبقرية التي قام بها بولسن عام 1990، مكّنته من السيطرة على كافة الخطوط الهاتفية التابعة لمحطة راديو محلية في لوس أنجلوس ضامناً بذلك أن يكون المتصل رقم 102 ليفوز بالجائزة الكبرى

وهي سيارة بورش 944 S2 بقيمة 50000 ألف دولار.

قد تبدو الاختراقات التي كانت تُشنّ في السبعينيات والثمانينيات والتسعينيات حسنة النية ضمن معايير اليوم. فعلى مر السنين، أصبح القراصنة في غاية التنظيم، وباتوا يشكلون تحالفات إجرامية عالمية على الإنترنت. فهم ينتحلون الهويات ويمارسون الاحتيال على البطاقات الائتمانية وعلى نظم الرعاية الصحية والشؤون الاجتماعية والضرائب. علاوة على ذلك، تضع عصابات الجريمة المنظمة نصب أعينها أهدافاً أكبر وأكثر تعقيداً، كالملكيات الفكرية الهائلة التي تخلقها الشركات في أنحاء العالم، من مخططات الإنتاج إلى الشيفرات المصدرية للبرمجيات. على سبيل المثال، استهدف قراصنة من أوساط الجريمة في تشرين الأول عام 2013 شركة أدوبي سيستيمز في وادي السيلكون، واستولوا على الأسماء وكلمات السرّ الخاصة بثمانية وثلاثين مليون حساب، بالإضافة إلى ملايين أرقام البطاقات الائتمانية. ولم يكن ذلك بالأمر الجديد، لكن الشيء المختلف في ذلك الهجوم هو أن المجرمين سرقوا أيضاً أكثر من أربعين غيغابايت من الشيفرة البرمجية الخاصة بمنتجات أدوبي الرئيسية، بما فيها برامج الفوتوشوب وكولدفيوجن وأكروبات.

نتيجة لذلك، أصبح بإمكان المجرمين لا فقط بيع منتجات أدوبي، بل وتعديل شيفراتها المصدرية لإقحام ما يحلو لهم من الأبواب الخلفية المخفية والبرمجيات الخبيثة وغيرها من الثغرات في هذه المنتجات، معرضين زبائن أدوبي الشرعيين غير المدركين للخطر إلى هجمات قرصنة وعمليات انتحال للهوية على نطاق واسع، وهو تطور مقلق بالفعل نظراً للانتشار العالمي الواسع لأدوبي بين مستخدمي الحاسب. وحتى شركة سيمانتك، صانعة برنامجي بي.سي.إنيوير ومضاد الفيروسات نورتون أنتيفايروس، سبق لها أن تعرضت لسرقة شيفرات مصدرية. أجل، الشركة التي تبيعك برنامج

مضادّ الفيروسات لتحميك من القرصنة، تعرضت بذاتها للاختراق حين سرق قرصان 1.27 غيغابايت من شيفرة برمجياتها الأمنية مطالباً بمبلغ تافه نسبياً بلغ 50,000 ألف دولار مقابل عدم نشر البيانات على موقع مشهور للقراصنة يعرف بـ "بايريت باي"، أو خليج القراصنة.

قامت عصابات الجريمة المنظمة التقليدية، كالمافيا الإيطالية وياكوزا اليابانية وعصابات المثلث الصينية، وعصابات تجارة المخدرات الكولومبية، بتحويل جهودها ومصادرها من النشاطات الإجرامية التقليدية نحو القرصنة الإلكترونية السهلة الربح وذات السرية العالية والأقل خضوعاً لمراقبة الشرطة. علاوةً على ذلك، لم يعد على هذه الجماعات بعد الآن أن تخشى الحدود الدنيا البالغة القسوة للأحكام التي عادة ما كانت تنجم عن نشاطاتها الاقتصادية السابقة، مثل تهريب المخدرات والإتجار بالبشر. فقد باتت عصابات الجريمة المنظمة الناشطة في الفضاء السايبري مسؤولة عن المضايقة برسائل البريد الإلكتروني والتصيّد ونشر الإعلانات الطبية المزيفة، وترويج الصور الجنسية المسيئة للأطفال وهجمات حجب الخدمة والابتزاز، إذا ما أردنا تسمية جزء يسير من نشاطاتها المفضلة.

إضافة إلى الحرس القديم القوي للجريمة المنظمة، ظهرت على الساحة فئة أكثر حذاقة من المنظمات الإجرامية الإلكترونية تهدف إلى التسلية فقط. تتمتع هذه التحالفات الإجرامية الجديدة الاحترافية التنظيم بربحية عالية وانتشار عالمي حقيقي، مع تركيز كبير لقواها في الصين وإندونيسيا والولايات المتحدة وتايوان وروسيا وبلغاريا والبرازيل والهند وأوكرانيا. بل إن بعض المنظمات الجديدة، مثل شبكة الأعمال الروسية في مدينة سانت بيترسبيرغ، قد كرست سمعتها كمنظمات جريمة سايبرية متعددة خطوط الإنتاج وبخدمات كاملة.

تشتهر شبكة الأعمال الروسية بتقديمها خدمة استضافة لمواقع الوب

"مضادة للرصاص"، توفرها لكافة أنواع المشاريع الإجرامية الأخرى، معتمدة سياسة عدم المسؤولية عن المحتوى الذي تستضيفه، مرحّبةً على مخدّماتها بأي شيء، ابتداءً بالمحتوى الإباحي للقاصرين وانتهاءً بعمليات تبادل البرمجيات الخبيثة. وثمة أيضاً مجموعات قرصنة إجرامية محترفة أخرى، مثل مجموعة شادوكرو، توفر ملاذاً إلكترونياً لـ "قراصنة البطاقات" المختصين بالعالم المظلم لوثائق الهوية المسروقة، كجوازات السفر ورخص القيادة المزورة وبطاقات الائتمان المسروقة، وهي المقومات الأساسية لاقتصادِ انتحال الشخصية العالمي المتنامي. وتدير مجموعة شادوكرو موقع المتوقف عن العمل حالياً، والذي كان يجمع أكثر من أربعة آلاف مجرم من كافة أنحاء العالم، يشترون ويبيعون الهويات والوثائق وأرقام الحسابات المسروقة بحرية. كانت عصابة شادوكرو، التي أسسها قرصان الجريمة المشهور ألبرت غونزاليس، تقدم دروساً تعليمية في الجريمة لزملاء الجريمة تعلمهم كل شيء، بدءاً من التشفير وصولاً إلى تقنيات استنساخ البطاقات. وكانت منظمة غونزاليس وفقاً للتقارير، مسؤولة عن سرقة وإعادة بيع أكثر من 180 مليون بطاقة ائتمان وصراف آلي. وقد ازداد عدد هذه الجرائم السايبرية المنظمة العابرة للحدود، ذات الربحية العالية، وتوسع نطاقها، وكانت شركة كراودسترايك الاستخبارية تقتفي أثر أكثر من خمسين منظمة رئيسية عالمية على هذه الشاكلة.

بالإضافة إلى منظمات الجريمة المنظمة العابرة للحدود، يمثل النشطاء - القراصنة إحدى أكثر الجماعات تأثيراً وقوة في الفضاء السايبري. فجماعات مثل أنونيموس ولولزسيك وأنتيسيك وويكيليكس والجيش الإلكتروني السوري تندرج تحت هذه الفئة، وكانت تشنّ هجماتها انتقاماً لظلم تشعر به. وقد أصبحت شخصيات مثل جوليان أسانج وتشيلسيا (برادلي) مانينغ وإدوارد سنودين أسماءً مألوفة لتحديها بعضاً من أكثر المؤسسات العالمية

قوةً، ولإطلاقها معلوماتٍ كان الكثيرون يفضلون بلا شك لو أنها بقيت مخفية. وبينما يظهر أسانج ومانينغ وسنودين على أغلفة الصحف حول العالم، تفضل مجوعات أخرى أن يبقى أعضاؤها بعيدين تماماً عن الأضواء وخاضعين فقط للمنظمة نفسها ولخططها الواسعة. ومجموعة أنونيموس هي أحد الأمثلة المميزة على ذلك، فهي منظمة تتحدث عن نفسها بنفسها ولا يوجد لها قائد، وأصبح أعضاؤها معروفين للعموم بارتدائهم أقنعة جاي فوكس.

يُظهر شعار المجموعة القائل "نحن الأنونيموس، نحن جيش. نحن لا نسامح. نحن لا ننسى. فتوقعونا"، الروح الجماعية المنظمة: "الفاسدون يخشوننا والشرفاء يدعموننا والنبلاء ينضمون إلينا". فعندما اتفقت شركات ماستر كارد وفيزا وباي.بال على إيقاف ضخ التبرعات لمنظمة ويكيليكس التابعة لجوليان أسانج، كانت ردة فعل أنونيموس بأن نفذت سلسلة من الهجمات الإلكترونية الفعّالة على هذه الشركات المالية. فمجموعة أنونيموس تعارض بقوة ما تعتبره قوانين جائرة لمكافحة القرصنة، وقد حصدت اعترافاً واسعاً بفضل هجوم سابق لها على شبكة بلي ستيشن من سوني كردةِ فعلٍ على دعم شركة سوني للقانون الأميركي المكافح للقرصنة والمعروف باسم: قانون وقف القرصنة الشبكية.

تعتبر مجموعة أنونيموس نفسها ناشطة في سبيل الخير، مستندة في ذلك على عدة أسباب اجتماعية، من ضمنها دعمها النشطاء في أنحاء الشرق الأوسط أثناء الربيع العربي. بل إن بعض ألدّ نقادها قد يجدون أنفسهم يدعمون بعضاً من نشاطات المجموعة الأقل شهرة في مكافحتها المنظمات الإجرامية والظلم. فأثناء الهجوم الذي أطلق عليه أوبيريشن داركنيت على سبيل المثال، استهدف عناصر من مجموعة أنونيموس موقعاً إلكترونياً إباحياً للقاصرين يحتوي على صورٍ وضيعة لقاصرين يُستَغَلّون جنسياً.

حيث قامت المجموعة بإخراج هذه المواقع من الشبكة ونشر أسماء ألف وخمسمئة من البيدوفيليين الذين كانوا يستخدمون خدمات الموقع. وسواءٌ أكان أحدنا يتفق أم يختلف مع أفعال مجموعة أنونيموس وغيرها من المنظمات الأخرى، فإن أمراً واحداً أصبح جلياً: إنهم قوةٌ لا بد من أن يحسب حسابها ضمن النسيج الواسع من الجهات الناشطة الخطيرة في عالمنا الشديد التشابك.

يستطيع النشطاء - القراصنة استهداف أي فرد أو شركة، ويمكن لهم أن يُحدثوا أثراً جيوسياسياً على العالم، كما جرى في الربيع العربي. فتقديراً لقوتهم المتنامية، قامت مجلة تايم بتصنيف أنونيموس كواحدةٍ من أكثر مئة شخصية مؤثرة في العالم عام 2012. ولم يخفَ على الحكومة تأثير المجموعة وقدراتها المتعاظمة، فقد تبين مؤخراً أن المركز الرئيسي للاتصالات الحكومية، وهو الرديف البريطاني لوكالة الأمن القومي الأميركية، قد أطلق هجمات حجب خدمة ضدّ مجموعة أنونيموس وأعضائها في محاولة لتعطيل نشاطاتهم. ويبين رد فعل الدولة المفاجئ على هذا النحو ضدّ مجموعة قرصنة فاعلة وغير حكومية التأثير الذي تتمتع به أنونيموس على العالم.

باتت المنظمات الإرهابية بدورها، تستخدم الإنترنت وغيرها من الأدوات التكنولوجية على نطاق واسع، لكي تخطط نشاطاتها الإجرامية وتدعمها وتنفذها. فالتكنولوجيا تساعد الإرهابيين على تجنيد أعضاء جدد من خلال غرف المحادثة السرية، وعلى تمويل عملياتها (عبر الجريمة السايبرية أو جمع التبرعات على الشبكة)، وعلى التواصل السري والدعاية، كما هو حال الفيديوهات المرعبة لعمليات ضرب أعناق الضحايا التي أنتجتها الدولة الإسلامية. وتتمتع الدولة الإسلامية بمعرفة تكنولوجية، وقد استغلت في فيديوهات التجنيد الأخيرة مشاهد معدلة من فيديو لعبة غراند ثيفت

أوتو V من أجل المؤثرات. وفي فيديوهاتها المتوفرة على الشبكة، تعرض عصابة الرعب المشؤومة على المجندين الجدد فرصة "القيام بأعمال مشابهة لما تقوم به في الألعاب، لكن في الحياة الواقعية وعلى أرض المعركة... كالهجوم على قافلة عسكرية أو قتل ضباط في الشرطة"، ويحمل الفيديو شعار الدولة الإسلامية.

أصبحت المعرفة بالإنترنت والبحث فيها أمراً مألوفاً لدى الإرهابيين، وقد حدث غير مرة أن عثر المسؤولون على صورٍ من موقع غوغل إيرث لأهداف مزمعة، مثل مخطط الهجوم الذي أعده إرهابيون عام 2007 لتفجير خزانات الوقود في مطار جون كينيدي في نيويورك. ولطالما كان الإرهابيون سباقين في الاعتماد على التقانة، وهم يستخدمونها خصيصاً في تشفير البيانات لحماية اتصالاتهم. فعلى سبيل المثال، استخدم "رمزي يوسف، وهو العقل المدبر المُدان بالتفجير الأول لمركز التجارة العالمي عام 1993، ملفات مشفرة ليخفي تفاصيل خطته لتدمير إحدى عشرة طائرة ركاب أميركية". وفي حالة يوسف هذه، استغرقت السلطة التنفيذية أكثر من سنة لكسر خوارزمية التشفير التي استخدمها الإرهابي. وهكذا كان الحظ هو وحده ما أسعف الشرطة في منع تنفيذ الخطة ضد الخطوط الجوية.

يعتبر بعض خبراء مكافحة الإرهاب الإنترنت "جامعة إرهابية"، فهي مكان يتعلم فيه الإرهابيون تقنيات ومهارات جديدة تجعل طرائقهم الهجومية أكثر فعالية. إذ تنتشر على الإنترنت وبشكلٍ كبير وثائق مثل "دليل المجاهدين في السموم"، والذي يحتوي وصفات متنوعة لصناعة السموم والغازات السامة في المنزل. وتتوفر أيضاً "موسوعة الجهاد"، المؤلفة من ستمئة صفحة أيضاً على الإنترنت بفصول متنوعة، مثل "كيف تقتل" و"الأجهزة المتفجرة" و"صناعة الصواعق" و"الاغتيال بواسطة الألغام". وفي مثالٍ واضح على الخطورة الناجمة عن مثل هذه المواقع التعليمية على

الإنترنت، اعترف دزهوخار تسارناييف، الإرهابي المشبوه والمعتقل لدوره في تفجيرات نيسان عام 2013 في سباق الماراتون في بوسطن، للسلطات بأنه تعلم مع أخيه كيفية صناعة قنبلة باستخدام قدر طبخ بالضغط، كالتي استخدمت في الهجوم، بعد قراءة التعليمات المفصلة الموجودة على موقع مجلة انسباير التابعة للقاعدة تحت فقرة بعنوان "اصنع قنبلة في مطبخ والدتك".

لم يقتصر استغلال الإرهابيين للإنترنت على دعم وتخطيط عملياتهم، بل إنهم لجأوا إلى القرصنة وجرائم الإنترنت كطريقة لتمويل وتنفيذ عملياتهم الإرهابية على أرض الواقع. ففي حزيران من عام 2007، تم تعطيل خلية بريطانية إرهابية إلكترونية على يد الشرطة، عندما اتُّهم ثلاثة مواطنين بريطانيين، هم طارق الداعور ووسيم موغال ويونس تسولي، باستخدام الإنترنت للتحريض على القتل. وقد أظهرت الأدلة المقدمة أن الثلاثة قد استخدموا حسابات بطاقات ائتمانية مخترقة لشراء موادّ يحتاج إليها زملاؤهم الجهاديون، ومن هذه المواد مثلاً مناظير للرؤية الليلية وأجهزة تحديد موقع وتذاكر طائرات وبطاقات مسبقة الدفع للهواتف النقالة. وكل ذلك بهدف توفير الدعم التكتيكي المباشر للعمليات الإرهابية. "وفقاً للتقارير، فقد حقق الثلاثة أرباحاً احتيالية بلغت أكثر من 3.5 مليون دولار أميركي، وكانت لديهم قاعدة بيانات تحتوي 40,000 حساب مسروق لبطاقات ائتمانية".

حتى العقل المدبر للتفجير الشائن في مدينة بالي عام 2002، وهو إمام سامودرا من عصابة الجماعة الإسلامية الإرهابية المرتبطة بالقاعدة، قام بتمويل هجومه الذي قتل فيه 200 شخص عبر 150,000 دولار حصل عليها عن طريق اختراق حسابات مصرفية وخطوط ائتمان غربية. كان سامودرا يتمتع بمعرفة تقانية واسعة، وكان قد كتب بياناً ذاتياً أثناء مكوثه في

السجن تضمّن جزءٌ منه العنوان، "القرصنة، لِمَ لا؟". في هذا الكتاب، بين سامودرا تقنيات الاختراق وقرصنة البطاقات لتابعيه، مشجّعاً إياهم على "الانتقال بالحرب المقدسة إلى الفضاء السايبري من خلال استهداف الحواسب الأميركية، وذلك لغرض محدد هو الاحتيال ببطاقات الائتمان لتمويل العمليات. ويبدو أن الرسالة قد وصلت للإرهابيين، فكلٌّ من تفجير مدريد الذي وقع في محطة أتوكا للقطارات عام 2004 مخلفاً 190 قتيلاً وحوالى 2000 جريح، وتفجيرات 7/7 في لندن التي راح ضحيتها 52 مدنياً وأصيب فيها أكثر من 700، تم تمويلها عن طريق القرصنة والاحتيال بالبطاقات الائتمانية.

مع تعاظم المهارات القرصنة التقنية لدى المنظمات الإرهابية، يزداد حجم الأرباح غير الشرعية التي يمكنها بلوغها عن طريق الإنترنت. ففي عام 2011، كشفت الشرطة الفيليبينية التي كانت تتعاون مع مكتب التحقيقات الفدرالي، عملية احتيالية تمت باختراقٍ هاتفي لشركة AT&T، تم من خلالها سلب مليوني دولار من الشركة وزبائنها. وكانت خلية القرصنة الفيليبينية تعمل مع مجموعة الجماعة الإسلامية، وقد أعادت ضخّ الملايين إلى جماعة إرهابية، كانت تمول بدورها جماعة لاشكار إيطَيبة المتمركزة في باكستان، وهي الجماعة الإرهابية المسؤولة عن الطوق التفجيري المميت الذي ضُرب عام 2008 على مدينة مومباي الهندية مسبباً قتل المئات وجرحهم.

بات واضحاً أن المجرمين والنشطاء - القراصنة والإرهابيين يستخدمون وسائل اتصالنا ضدنا، سواء في سبيل المنفعة أو السياسة أو القتل. فقد ثقفوا أنفسهم في مجالات العلم والتقانة وأظهروا قدرات مرعبة في استغلال الأسس الهشّة بطبيعتها التي تقوم عليها القشرة التقانية في القرن الحادي والعشرين. إلا أن اللصوص والقراصنة والنشطاء والإرهابيين ليسوا

الوحيدين في الأوساط السرية الرقمية، بل ترافقهم كتائب جرارة من الدول القومية ومحاربي الإنترنت وأجهزة الاستخبارات الأجنبية، التي يؤدي كل منها دوره ببراعة فيما يُسمى بالبعد الخامس، حيث يستغلون هشاشة البنية التحتية الرقمية التي توحّد العالم استغلالاً كاملاً لأجل مصالحهم الخاصة.

على الرغم من أن مُستخدم الإنترنت العاديّ اليوم، قد يكون مشغولاً بتحديث حالته على الفايسبوك أو بممارسة لعبة الطيور الغاضبة، فإنه من الضروري ألاّ ننسى أن الإنترنت الحالية قد ولدت على يد وكالة مشاريع أبحاث الدفاع المتقدمة (داربا)، وهي اختراع لوزارة الدفاع الأميركية أُحدِث لضمان استمرارية الاتصالات العسكرية في حالة التعرض لهجوم نووي، أي إن الإنترنت هي اختراعٌ عسكري تلازمه تشعبات جيوسياسية لا يستهان بها.

فقط عندما تصب الحكومات اهتماماتها (وميزانياتها) على عمليات إلكترونية هجومية، يُمكننا ملاحظة مدى هشاشة الأجهزة والبرامج التي نعتمد عليها ويتكشف لنا الضعف التقاني الذي نعانيه. فمع أن عملية ابتزاز إجرامية بمقدار 50,000 دولار تعرضت لها سيمانتك أو حتى خسارة بليون أو بليوني دولار نتيجة هجومٍ إلكتروني على هدفٍ معيّن تبقى جديرة بالاهتمام والاعتراف، فإنها ليست سوى تغيّر تافه إذا ما قورنت بعملية الاختراق والتجسس التي طالت حواسب مشروع طائرات إف 35 في البنتاغون بميزانيته المقدرة بـ 300 بليون دولار تجعله أغلى برنامج أسلحة تشهده وزارة الدفاع عبر التاريخ.

ففي شهر أيار عام 2013، اعتبرت الحكومة الأميركية أن الصّين تحديداً هي المسؤولة عن سلسلةٍ من الاختراقات التي استهدفت أنظمة دفاعية وحكومية حيوية من بينها طائرات إف 35. فقد كانت التقارير ترد على مدار السنين المنصرمة مفيدة بسرقة العديد من المخططات والتقنيات

الدفاعية الأخرى، من ضمنها نظام صاروخ الباتريوت المتقدم باك3، ونظام البحرية الدفاعي المضاد للصواريخ البالستية، ومقاتلات إف/إيي 18 و-V 22 أوسبري وطائرات بلاك هوك العمودية، والسفن الخاصة بمعارك السواحل. ووفقاً لتقرير صادر عن مكتب التحقيقات الفدرالي، قامت الصين سرًّا بتطوير جيشٍ قوامه 180,000 جاسوس ومحارب إلكتروني، ينفذون كل سنة تسعين ألف هجوم حاسوبي ضد شبكات وزارة الدفاع وحدها. أما إجمالي السرقات وأثرها على الأمن القومي الأميركي فهي تدعو إلى الصدمة.

تعود هذه النشاطات الهجومية الإلكترونية المزعومة على الصين بفوائد استراتيجية هامة، من بينها التفوق التكتيكي والعملياتي المباشر في أي صراعٍ مع الولايات المتحدة. إذ يوفر الاستحواذ على المخططات الخاصة بأنظمة الدفاع الأميركية التفاصيل الرئيسية لكيفية عملها، وإمكانيات هزيمتها في فترات الأزمات. كما أن هذه "السرقة الفكرية" توفّر على الصين بلايين الدولارات وسنواتٍ من العمل من ميزانيتها للأبحاث العسكرية، إذ يصبح بإمكانها استغلال العمل الذي تكبّد تكاليفَه دافعو الضرائب الأميركيون والبناء عليه.

لم تكن التكنولوجيا العسكرية الأميركية وحدها المستهدفة من قبل الصين على أية حال، فثمة أيضاً مجموعة من المؤسسات في العاصمة واشنطن، من بينها شركات قانونية ومراكز أبحاث وجماعات حقوق إنسان ومقاولون ومكاتب في الكونغرس وسفارات وعدد من الوكالات الفدرالية. علاوةً على ذلك، كشف تقرير صدر عن باحثين كنديين في مركز مراقبة معارك المعلومات وجماعة سيكديف ومركز الأبحاث الوطني في جامعة تورونتو عام 2009 عمّا يُسمّى شبكة الأشباح، وهي "شبكة تجسس إلكترونية واسعة"، تمتد عبر 103 بلدان تتحكم بها مخدمات مقرها في الصين، كانت قد استهدفت حكومة المنفى التبتية وقائدها الدالي لاما بالذات.

اتُّهمت الصين أيضاً باختراق منافذ إعلامية عديدة، أشهرها صحيفة نيويورك تايمز في بداية عام 2013 بعد أن أصدرت الصحيفة تقريراً مفاده أن أقارب رئيس الوزراء الصيني، وين جياباو، جمعوا ثروةً تقدر بمليارات الدولارات من خلال تعاملاتهم التجارية منذ أن تسلّم وين منصبه. وتمكن المنفذون من خلال هذا الاختراق من الوصول إلى أي حاسبٍ تابعٍ لشبكة نيويورك تايمز، وكان يُعتَقد أن الصينيين كانوا يعملون على كشف المصادر والاتصالات التي قد تضر بسمعة القادة الصينيين. واستعانت التايمز بشركة أمنية إلكترونية خاصة تُدعى مانديانت، قامت بالتحقيق في الحادثة وأصدرت تقريراً مدهشاً ربطت فيه الهجوم بالوحدة 61398 التابعة لمجموعة جيش التحرير الشعبي. ويقع مركز قيادة هذه الوحدة في شارع داتونغ رود في مقاطعة بودونغ التابعة لولاية شانغهاي، وتبلغ مساحته 13 قدم مربع، ويشتمل على بناء من اثني عشر طابقاً يداوم فيه يومياً آلاف الموظفين الذين يعملون على اختراق شبكات الحكومات والشركات والأفراد في أنحاء العالم.

لا تُنفّذ هذه السرقات التكنولوجية الدولة الصينية مباشرة، لكنها تتم تحت رعايتها وعن طريق وكلاء، وهي تؤدي إلى تكاليف كبيرة وآثار عميقة تصيب الأعمال في أنحاء العالم. ففي عام 2012، قامت مجلة بلومبرغ بيزنيس ويك بتغطية سرقة الصين المستمرة للممتلكات الفكرية العالمية، حيث وضعت على غلافها عنواناً صارخاً وبالأحرف العريضة "أيتها الصين، توقفي عن سرقة أشيائنا". وكان موضوع العدد هو قصة دان ماك.جان، المدير التنفيذي للشركة الأميركية للنواقل الفائقة في ماساتشوستس، وهي شركة تكنولوجية مختصة بالطاقة النظيفة وتُعنى بتصميم أنظمة الطاقة والبرامج التي تشغل توربينات الرياح الكبيرة. ففي آذار من عام 2011، بدأت مجموعة سينوفيل ويند الصينية التي تمتلكها الدولة، وهي أحد أهم

زبائن الشركة الأميركية، فجأةً برفض شحنات مصنع التجميع الخاص بها في مقاطعة ليانونغ، وألغت ما قيمته أكثر من 700 مليون دولار من الطلبيات المعلّقة. وكانت استجابة السوق على إلغاء هذه الطلبيات مرعبة، فقد هبطت القيمة التقديرية للشركة بمعدل 40 بالمئة في يومٍ واحد وتراجعت المبيعات بنسبة 84 بالمئة بحلول شهر أيلول من ذلك العام.

أظهر تحقيق في تلك الحادثة أن المحركات الخاصة بسينوفيل "يتم تشغيلها باستخدام نسخة مسروقة من برامج شركة (AMSC)"، وأن الشركة الصينية انتزعت نسخة كاملة من الشيفرة المصدر لبرمجيات الشركة الأميركية. ومع حيازة سينوفيل كافة الممتلكات الفكرية لشركة (AMSC)، لم تعد بحاجةٍ إلى الشركة ومنتجاتها، بل بات بإمكانها أن تنتج المنتجات نفسها التي تنتجها الشركة الأميركية. وكانت النتيجة أن ألغت الشركة الصينية عقود التوريد القائمة مع شركة ماساتشوستس والبالغة قيمتها أكثر من 700 مليون دولار.

وهكذا فإن الجهود المتواصلة المبذولة في مجال القرصنة والاختراق الإلكتروني، من خلال سرقات الممتلكات الفكرية التجارية والحكومية والعسكرية، عادت على الأمة الصينية بأكبر عملية نقل للثروات في التاريخ البشري. فوفقاً لتقرير حالة الإنترنت التي تعده أكاماي، تمثل الصين مصدراً لنسبة صادمة من الهجمات الإلكترونية في العالم تبلغ 41 بالمئة.

أما الصين، فلا تنفك بالطبع تنكر علاقتها بأية نشاطاتٍ تتعلق بالقرصنة الإلكترونية العالمية إنكاراً قاطعاً. وعندما كانت تُثار المزاعم، عادة ما كانت الأجوبة المكررة تصدر عن المتحدث الرسمي باسم السفارة الصينية في عاصمة البلد المعني، سواءٌ كانت باريس أو برلين أو نيودلهي. ففي رسالة صادرة عن موظف في السفارة الصينية في واشنطن العاصمة، ويُدعى وانغ باودونغ جاءت الإجابة المعتادة: "تؤكد الصين وبشدة أنها ضد نشاطات

القرصنة العالمية، كما أنها على استعداد للعمل مع كافة الدول لتأمين الفضاء السايبري". ولم يكن هذا الإنكار من قبل وانغ هو الأول من نوعه، فعملية بحث في موقع غوغل عن عبارة "الصين تنكر القرصنة" ستتمخض عن خمسةٍ وثلاثين مليون استنكارٍ مشابه.

على الرغم من أن الصين أكثر دولة مزدحمة في العالم، فإنها ليست البلد الوحيد المتورط في عمليات سايبرية. فتبعاً للمدير السابق لمكتب التحقيقات الفدرالية، روبرت مولر، ثمة أكثر من 108 دول لديها وحدات مكرسة للهجمات السايبرية تسعى وراء الأسرار الصناعية والبنى التحتية الهامة، ومن بينها إيران. ففي أواخر عام 2012، أعلنت مجموعة لم تكن معروفة من قبل اسمها "سيف العدالة القاطع"، مسؤوليتها عن تنفيذ عملية التخريب الحاسوبية الأكثر تدميراً في التاريخ، والتي طالت حواسب الشركة السعودية للنفط والغاز آرامكو. وقد حدث الهجوم في ليلةٍ تُعدّ من أقدس الليالي بالنسبة للمسلمين وهي ليلة القدر. وكان موظفو الشركة البالغ عددهم خمسة وخمسين ألف موظف في بيوتهم يحتفلون بهذه المناسبة مع عائلاتهم وأصدقائهم. وكان على المحكّ مصير 260 بليون برميل نفط تبلغ قيمتها أكثر من 8 تريليون دولار (وهي قيمة أكبر بأربع عشرة مرة من القيمة التسويقية لشركة أبل).

خلال الحادث، قام شخص مجهول من الداخل، يمتاز بصلاحية الوصول إلى المنشأة بإدخال قرص يو.إس.بي مصاب في جهاز حاسب موصول بشبكة حواسب الشركة. وفي غضون دقائق، كانت الحمولة الفيروسية الموجودة على السواقة، والمعروفة باسم شامون، تنتشر مثل النار في الهشيم عبر جميع أجهزة الحاسب لشركة آرامكو، والبالغ عددها ثلاثين ألفاً. وعلى الرغم من أن الهدف كان تعطيل إنتاج النفط والغاز في جميع مرافق آرامكو، فإن الإجراءات الأمنية الجيدة قضت بأن يدمّر الفيروس بيانات

الشركة فقط. أما الحصيلة، فكانت قيام شامون بمحو 75 بالمئة من سواقات الحواسيب الثلاثين ألفاً، حيث مسح "الوثائق وجداول البيانات ورسائل البريد الإلكتروني والملفات - واستبدلها جميعاً بصورةٍ للعلم الأميركي وهو يحترق".

أعلنت جماعة سيف العدالة القاطع أن هجومها هذا جاء رداً على سياسة السعودية ضد المعارضين الشيعة في سوريا والبحرين. ويشتبه مسؤولو الاستخبارات الأميركية بأن تكون جماعة سيف العدالة القاطع مجرد واجهة لإيران، التي في الحقيقة هي من يجب أن يلام لرعايتها هذا الهجوم. فهذه القدرات المفاجئة التي برزت من خلال هجوم آرامكو سبقها العديد من الهجمات الناجحة التي نفذتها الحكومة الإيرانية، من بينها سلسلة من هجمات حجب الخدمة الموزعة في بداية عام 2013 استهدفت مرافق الصناعة المالية في أميركا، ومن بينها العديد من البنوك المشهورة مثل جي.بي.مورغان تشيز وبنك أميركا وويلز فارغو وبي.بي.آند.تي (BB&T) ومصرف إتش.إس.بي.سي وسيتي غروب، حيث عطل الهجوم الوصول إلى شبكاتها ومواقعها الإلكترونية العامة لفترات طويلة منع خلالها الزبائن الحصول على أموالهم. وأعلنت جماعة من القراصنة تُسمّي نفسها محاربي عز الدين القسّام الإلكترونيين مسؤوليتها عن هذا الهجوم الخاطف، لكنّ الموظفين الأميركيين قالوا إن الجماعة ليست سوى وكيل لإيران.

كان هجوم حجب الخدمة الإيراني الواسع الذي استهدف الصناعة المالية الأميركية، مفاجئاً بحجمه ونطاقه وبالكم الهائل من البيانات التي خلفها الجُناة. فقد تعرضت بعض البنوك لفيضٍ متواصلٍ من الحركة بلغت ذروتها 70 غيغابايت في الثانية الواحدة. ولنتصور هذا الكم من عمليات النقل الهادفة إلى حجب الخدمة، يمكننا تشبيهه بقيام بليون شخص في الوقت نفسه بالاتصال بالبنك وإغلاق الاتصال ليعودوا مباشرة للاتصال بعد ثانية

واحدة. فلكي تتمكن أنت من إجراء مكالمتك (أو من زيارة الموقع الإلكتروني) سيكون رقمك الواحد بعد البليون على القائمة. بعبارة أخرى، لن تتمكن من الوصول إلى البنك مهما كان غرضك.

أما ما يصدم في الأمر، فهو أن الهجوم الإيراني المُحكم ضد قطاع الخدمات المالية بحسب التقارير، أكبر بعدة مرات من الهجوم الشائن الذي استهدف استونيا عام 2007، والذي نفذه قراصنة يتخذون من روسيا مقراً لهم. وهو الهجوم الذي وضع البلد البلطيقي الصغير خارج الشبكة تماماً. فمن المعتَقد أن الحادثة نُفذت بدعم مباشر من الحكومة الروسية وعن طريق قراصنة وكلاء قوميين، بعد أن قررت استونيا نقل نصب تذكاري يعود للحقبة السوفييتية من مكانه القديم في مركز مدينة تالين إلى ضاحية المدينة في تصرف أغضب موسكو كثيراً.

أطلق العديد من الخبراء الأمنيين على هذا الهجوم الرقمي الشامل الذي تعرضت له استونيا لقب "الحرب العالمية الإلكترونية الأولى"، وذلك نتيجة حجم هذا الهجوم ونطاقه. ونظراً لتفوق الهجوم الإيراني على هذا الهجوم، أشار أحد الباحثين الأمنيين إلى أن القصف التقاني للجمهورية الإسلامية لم يعد "مجرد عواء بعض كلاب الشيواوا أمام مجموعة من الديناصورات النافثة للنيران".

كانت ثمة أيضاً مزاعم كبيرة عن قيام الولايات المتحدة بأعمال قرصنةٍ ضد بقية أنحاء العالم بالطبع، وهي مزاعم تستند إلى العديد من الوثائق السرية المسروقة، والتي نُشرت من جانبٍ واحد عن طريق مقاول في وكالة الأمن القومي يُدعى إدوارد سنودين، كان قد باشر في عملية النشر في شهر حزيران عام 2013. فقد قدّم سنودين تفاصيل طويلة عن جهاز المراقبة التقنية العالمي الذي تديره وكالة الأمن القومي، داعماً ادعاءاته بأدلة وثائقية في مناقشةٍ جرت مع كلٍّ من الصحافييّن غلين غرينوالد ولاورا

بويتراس. وما لبثت أن ظهرت تباعاً برامج أخرى مثل برنامج بريزم وإكس كيسكور، وكذلك ظهرت إلى الأضواء قدرة وكالة الأمن القومي المزعومة على تتبع مليارات رسائل البريد الإلكتروني والرسائل الهاتفية وجلسات المحادثة والرسائل القصيرة في كل يوم.

أثناء مكوثه لفترة وجيزة في موسكو كلاجئ سياسي، تابع سنودين تصنيف العمليات الهجومية الإلكترونية والتقنية للولايات المتحدة، بما فيها تسجيل المكالمات الهاتفية الخلوية الخاصة بعدد من قادة العالم، بدءاً بالمستشارة الألمانية أنجيلا ميركل ووصولاً إلى الرئيسة البرازيلية ديلما روسيف. وأفشى سنودين سراً مفاده أن الملايين من المواطنين في البلدان الحليفة لأميركا، مثل فرنسا وألمانيا، قد تعرضت اتصالاتهم للتسجيل، بما يعادل 120 مليار مكالمة في الشهر في أنحاء العالم.

أسهمت التسريبات التي قدمها سنودين في الحد من التعاطف الدولي مع الاتهامات الأميركية، المتعلقة بالهجمات الإلكترونية العديدة التي تعرضت لها على يد جمهورية الصين الشعبية، خاصةً عندما كشف أن الولايات المتحدة أيضاً أطلقت عملياتٍ إلكترونية ضد أهدافٍ صينية من بينها شركة الصين للاتصالات الخلوية وجامعة تشنغهاو الرفيعة المستوى. ووفقاً لاعتقادات المرء السياسية ووجهات النظر الفردية، قد يعتبر سنودين عدواً للدولة أو بطلاً أو ناشطاً محذراً أو مشاكساً أو خائناً أو وطنياً. لكن معظم الناس يميلون إلى إحدى هذه الصفات فقط. وبغضّ النظر عن كيفية تقييم التاريخ لسنودين، فإن تسريباته الفاضحة، إذا ثبتت صحتها، تكون قد رسمت صورة مفصّلة عن كيفية دخول الحكومات في صراع سايبري.

يُظهرُ تحليل مصادر التهديدات في الفضاء السايبري أنه يشتمل على القراصنة والمجرمين والمحاربين بالوكالة والإرهابيين والحكومات المارقة، وكلهم قادرون على استغلال هشاشة البنية التحتية التكنولوجية لعالمنا.

فبياناتنا المالية وهوياتنا وصور أطفالنا وهم صغار وشبكات الطاقة لدينا، كلها حساسة وعرضة للخطر، وهي تمثل أهدافاً سهلة. لكن مهما بدت التقانة كلية الوجود في حياتنا اليوم، فإن معدل النمو الأسّي يعني وجود موجة مدّ من التطورات التكنولوجية تلوح في الأفق، قادمة إلينا لتجعل رؤوسنا تدور. فعمق اتصالنا بشبكة المعلومات العالمية ليس وحده الذي سيزداد، بل ستبرز معه تقانات جديدة لطالما صنفت في نطاق الخيال العلمي لتصبح من ثمّ حقيقة علمية. باختصار، لم نر شيئاً بعد.

الفصل الثالث
الجريمة الخاضعة لقانون مور

لقد وصلنا المستقبل بالفعل، لكنه لم يوزّع بشكل عادل بعد.

ويليام جيبسون، من مدونة نويرومانسر

لكي يتعلم تلامذة المدارس في فرنسا الطاقة الرياضية للأس وللمنحنيات الأسّية، كان يطلب إليهم تخيل بركة تنمو على سطحها ورقة زنبق مائي صغيرة. تنمو هذه الورقة مضاعفة حجمها، كما قيل للتلاميذ، وتستغرق ثلاثين يوماً حتى تغطي البركة كلها. لكنها إذا غطت البركة كلها فستخنق جميع أشكال الحياة الأخرى في الماء وتقتلها. وكان السؤال الذي طرح على التلاميذ حينها هو عن اليوم الذي ستغطي فيه الورقة نصف مساحة البركة.

لم يكن في البداية ثمة ما يقلق، فقد كانت ورقة الزنبق تنمو بمعدل بالكاد يمكن ملاحظته لتغطي عشر الواحد بالمئة من سطح البركة في اليوم العشرين، أي 0.1 بالمئة فقط. لكنها بعد ثلاثة أيام باتت تغطي ثلاثة بالمئة. نظراً لضآلة هذه النسبة أيضاً، تابع التلاميذ نمو الورقة إلى أن صارت فجأة، في اليوم 29، تغطي نصف البركة. في ذلك اليوم، لم يكن قد بقي الكثير من الوقت لإنقاذ البركة التي ستخنقها الزنبقة في اليوم التالي. قد يبدو اليوم التاسع والعشرون يوماً عادياً كسائر الأيام في معظم الأحيان، لكن طبيعة الأعداد الأسّية تعني أن البركة كانت محكومة مسبقاً بالموت.

أما الدرس المستقى من مسألة البركة فهو عن الطبيعة السحرية للنمو الأسّي وكيف أنه يتسلل بسرعة هائلة بينما نستمر نحن في تفكيرنا الخطي مجازفين بأنفسنا.

عالم النمو الأسّي

في كتابه "الفردية تقترب"، يصف عالم المستقبليات ريي كورتسفايل

الطبيعة الأسّية للعالم التقاني الذي يحيط بنا، مقدماً مفهوماً دعاه "ركبة المنحني الأسّي". وركبة المنحني هي نقطة انعطاف زمنية يصبح عندها المسار الأسّي واضحاً بالفعل. ثم لا يلبث المنحني أن يصبح انفجارياً ذا منحى عمودي صاعد يبين الأثر الرياضي للنمو الأسّي. وربما كان مالكولم غلادويل سيصف هذه الظاهرة بأنها "نقطة الانقلاب"، التي يؤدي عندها اجتماع العديد من الأشياء إلى إحداث فرق كبير ملحوظ في النتائج. ونظراً للطبيعة الأسّية للتقانة ووجودها الشامل في حياتنا، ثمة دليل لا يدحض على أننا نقترب بسرعة من نقطة انقلاب. ويبقى السؤال هو ما إذا كان هذا الانقلاب لصالحنا أم لا.

وفقاً لاتحاد الاتصالات العالمي، لم يكن هناك عام 2000 سوى 360 مليون شخص متصل بالإنترنت. ومع أن ذلك التطور كان قد استغرق 40 عاماً، فإن تعداد هذا الوسط العالمي للمتصلين وصل عام 2005 إلى مليار شخص لأول مرة. أما المليار الثاني فانضم في غضون ست سنوات تلت، حين تحقق هذا الرقم في آذار من عام 2011. وكان النمو الأعظم في العالم النامي حين كانت آسيا وأفريقيا تحققان تصاعداً صاروخياً بنسبة 842 بالمئة و3606 بالمئة بالترتيب اعتباراً من عام 2000. وبينما نصف العالم غير قادر للأسف على الوصول إلى الإنترنت اليوم، فإن عضو مجلس الإدارة التنفيذية في غوغل، إيريك شميدت، تنبأ بشجاعة بأن كل فرد سيكون متصلاً بالإنترنت بحلول عام 2020.

كان الإيقاع الذي لا يخبو لهذه التغييرات والحضور المتنامي دائماً للتقانة في حياتنا، محكومين بإحدى مسلمات التقانة المعروفة باسم قانون مور. وهو مفهوم سمّي تيمناً بغوردون مور، عضو الإدارة السابق في شركة إنتل، والذي عرف عام 1965 بأنه تنبأ بتضاعف عدد الترانزستورات في البوصة المربعة من الدارات متكاملة كل عام في المستقبل. يشار إلى هذا القانون،

الذي شُذِّب في ما بعد بحيث يكون التضاعف كل 18 شهراً إلى سنتين، باسم قانون مور، وهو يطبق اليوم على نطاق أوسع ليشمل طاقة وقدرات جميع التقانات المعتمدة على الدارات. لذا فإن طيفاً جديداً من الاكتشافات العلمية، من التقانة الإحيائية إلى الروبوتيات، يحكمه قانون مور وتبعاته. فلقانون مور أيضاً تبعات تتجاوز العلم، وتتراوح من الجيوسياسة إلى الاقتصاد لأن جميع جوانب الوجود الإنساني تزداد ارتباطاً بالتقانة. ولا يجوز نسيان أن قانون مور قد يكون له تبعات سلبية أو إيجابية على عالمنا.

إن المضاعفة المستمرة لقدرة الحواسب على المعالجة، والمحكومة بقانون مور، هي التي تمنح تأثيره كل هذا العمق. فهي تعني أن منحنيات النمو الخاصة بجميع التقانات المعتمدة على الحواسب هي منحنيات أسّية لا خطية. بعبارة أخرى، لا تستفيد هذه التقانات من طاقة الجمع فقط، بل من طاقة الضرب. وهو الفرق بين سلسلة 1، 2، 3، 4، 5، 6، 7 و1، 2، 4، 8، 16، 32، 64، 128. وكلما استمر المنحني الأسّي في مساره مقابل المنحني الخطي، كانت النتائج واضحة وصادمة. ولكي نضع هذا المفهوم في إطاره الصحيح، فإننا إذا ما قمنا بثلاثين خطوة خطية، لأمكننا السير عابرين الغرفة. لكن ثلاثين خطوة أسّية، أي مضاعفة المسافة المقطوعة مع كل خطوة، تعادل قطع المسافة بين الأرض والقمر. إن إدراك هذه الطبيعة الأسّية، لا الخطية، لمنحنيات نمو تقانات اليوم هي الأساس المطلق لفهم المرحلة القادمة للتطور البشري. فنحن اليوم نعيش في عصر أسّي.

مع استمرار تقانة المعلومات في مضاعفة أدائها السعري وقدراتها وعرض الحزمة الذي توفره، ستصبح أشياء مدهشة جزءاً من الواقع. ولنأخذ على سبيل المثال هاتف الآيفون الذي يحمله مئات الملايين من المستخدمين في جيوبهم، فمن الصعب تصديق أنه يحمل من طاقة المعالجة الحاسوبية،

حرفياً، أكثر مما كان متوفراً لدى وكالة ناسا كلها خلال عملية الهبوط على القمر الذي نفذته مركبة أبولو 2 قبل أربعين عاماً. الهاتف الذكي الحديث "أرخص بمليون مرة وأسرع بألف مرة من الحواسب الفائقة التي كانت موجودة في السبعينيات". لكن نظراً للتبعات الرياضية للأس ولقانون مور، فإننا "لا نعيش تقدم مئة عام في القرن الحادي والعشرين، بل سيكون الأمر أشبه بتقدم عشرين ألف سنة (بمعدل التطور الحالي)".

نظراً للوتيرة الأسّية للتغيير في طاقة المعالجة في الحواسب وفي تعقيدها، من الواضح أن الحواسب ستمتاز بقدرات هائلة في المستقبل القريب. يصف راي كورتسفايل المضاعفة المستمرة للأداء السعري للحواسب وطاقتها في قانونه الخاص بالـ "العوائد المتسارعة". إذ يتنبأ بلحظة زمنية تحدث فيها الفردية التقانية، أي اللحظة التي يكون فيها التطور الحاسوبي من السرعة، بحيث يتجاوز قدرة البشر على استيعابه وتتجاوز الآلات في ذكائها ذكاء الإنسان. وسواءٌ كان هذا اليوم سيأتي أم لا (وكورتسفايل يتوقع أن يكون عام 2045)، فإن الواضح هو شيء واحد: بينما تنمو الطاقة الحسابية أسّياً، تتضاءل قدرتنا على فهم شبكة المعلومات العالمية وخريطة اتصالاتها البينية الهائلة.

ليس هذا مجرد خيال، فالتقانة تتقدم بالفعل بوتيرة يعجز معظمنا عن مواكبتها، والذنب ليس ذنبنا. فقد فرض تطور البشر عليهم أن يفكروا بطريقة خطية مبرمجة في أدمغتهم منذ فجر الجنس البشري. فنحن نجري الحسابات الخطية فطرياً في أدمغتنا منذ كنا في سهوب سيرينغيتي، حين كنا نحاول تحديد أفضل مسار نهرب عبره من أسد هائج. لكن هذا لم يعد هو العالم الذي نعيش فيه اليوم. بل إن كورتسفايل يعتقد أن السنوات القادمة ستحمل معها "تغيراً تقانياً سريعاً وعميقاً إلى درجة تجعله يمثل تمزقاً في نسيج التاريخ البشري". فإذا نظرنا إلى معدل التغيير المتسارع أبداً والرحلة

التي قمنا بها من الحواسب التي تحتل بناءً كاملاً إلى هواتف آيفون خلال السنوات الأربعين الماضية، فما الذي تحمله لنا السنوات الأربعون القادمة؟ قدراً أكبر بكثير من الخير، لكن ربما قدراً أكبر بكثير من الشر أيضاً، أكثر مما يمكن لمعظمنا تخيله.

ليست المسألة ثنائية بسيطة حول ما إذا كانت التقانة جيدة أم لا، بل هي مسألة عوائد متسارعة. فكيف لنا أن نبقى في مأمن في عالم يتحرك بهذه السرعة؟ نحن نقوم ببناء حضارة ذات اتصالات بينية عميقة، لكنها تقانة غير آمنة في الوقت نفسه. بعبارة أخرى، إننا نبني عالماً مهيئاً للجريمة ومرتعاً للتهديدات الأمنية الأخرى. وثمة أدلة متزايدة تشير إلى هذه الأخطار وتظهر لنا صنفاً جديداً ناشئاً من النخب الإجرامية والإرهابية ومن الحكومات الأجنبية التي تستغل هذه التقانات لمصلحتها. النتيجة؟ إننا نجد أنفسنا نزداد تواصلاً وتبعية ونقاط ضعف.

فردية الجريمة

كانت الجريمة ذات يوم مسألة بسيطة. فكان بإمكان أي شخص أن يصبح مجرماً بمجرد أن يبتاع سكيناً أو بندقية ويلبث في ممر معتم ليخرج من مكمنه حين تقترب الضحية مطالباً إياها بـ "أعطني نقودك". وبعيداً من المسألة الأخلاقية، كان السطو نموذج مشاريع تجارية عظيماً استمر طوال ألفية كاملة. فكانت تكاليف الشروع منخفضة، وكان بإمكان المجرمين العمل أو الاستراحة وفق توزيع الساعات والبرامج التي تحلو لهم. وعلى غرار جميع أصحاب المشاريع، كان على المجرمين أن يتقبلوا مشكلة واضحة: كيف يمكن تحقيق التوسع والنمو في مجال عملهم. فحتى السارق الجيد لا يتمكن من سلب أكثر من خمسة أو ستة أشخاص في اليوم، هذا إذا حالفه الحظ.

لكن التقانة، لحسن الحظ، ما لبثت أن قدمت الحل لمن يريد أن يصبح

مجرماً، بحيث يتغلب على عقبات التوسع التي تقف في طريق أعماله المحظورة، وجاء هذا الحل من مكان لم يكن متوقعاً: القاطرة. فحين اخترعت القطارات، لم يكن أحد يتخيل بالطبع أنها قد تصبح هدفاً للصوص القطارات. لكن المجرمين، على أية حال، تنبؤوا بهذه الفرصة السانحة ولم يضيعوا وقتاً، بل سارعوا إلى استغلال التقانة الجديدة. وصار بإمكان المسلحين عندها، بدلاً من نهب شخص واحد في كل مرة، وبفضل القاطرات، أن ينهبوا مئتي أو ثلاثمئة شخص في آن معاً، موسعين فرصهم التجارية وأرباحهم.

تمكن متعهدو الجرائم الأوائل من أمثال بيل ماينر وجيس جيمس وبوتش كاسيدي، في منتصف إلى نهاية القرن التاسع عشر، من جني ثرواتهم من خلال السطو على القطارات وحمولاتها ومسافريها وما يحملونه من المال والمجوهرات. وبقيت الهجمات على القطارات شكلاً قائماً من أشكال العمالة الإجرامية لمدة تزيد على المئة عام وصلت إلى ذروتها في عملية السطو الكبيرة في المملكة المتحدة عام 1963، حين تمكنت عصابة من اللصوص من السيطرة على قطار ملكي متوجه من غلاسغو إلى لندن. وعادت الغزوة المخططة بإحكام على الطاقم بـ 2.6 مليون جنيه استرليني، تعادل اليوم 64 مليوناً (7.28 و76 مليون دولار على الترتيب).

إذا قفزنا بالزمن إلى عالم اليوم، فسنرى أن بإمكان الجريمة أيضاً أن تستفيد من الطبيعة الأسّية للتقانة. فباستخدام الإنترنت، انتقل اللصوص من السطو على الأفراد أو على المئات من الأشخاص دفعة واحدة إلى سرقة الآلاف، بل والملايين، من الأفراد اليوم. لذا فإننا نشهد اليوم تحولاً منهجياً عميقاً في طبيعة الجريمة وطريقة تنفيذها. فالجريمة تتوسع أسّياً، حالها في ذلك حال التقانة.

كما نوهنا سابقاً، كانت عملية السطو التي نفذها تي.جي. ماكس أكبر

جريمة تجزئة من نوعها في ذلك الوقت، حيث طالت في البداية البيانات المالية لـ 45 مليون زبون. لكن عناوين الصحف لم تدع مجالاً للشك في أن الحادثة لم تكن حادثة فردية. ففي شهر تموز من عام 2011، تمكن مهاجمون من اختراق شبكة ألعاب البليستيشن لدى سوني وتمكنوا من الوصول إلى أكثر من 77 مليون حساب شبكي تحتوي على أرقام البطاقات الائتمانية للزبائن وأسمائهم وعناوينهم وتواريخ ميلادهم وبيانات دخولهم إلى شبكة الألعاب. واضطر الهجوم شبكة بليستيشن إلى التوقف عن الخدمة لعدة أيام ليتأثر بذلك ملايين المستخدمين في أنحاء العالم. ولم يُضِع المجرمون وقتاً، بل راحوا يستغلون وسائل الراحة التي توفرها التقانة في حياتنا، بما فيها منصات الألعاب. وقدر المحللون الماليون في نهاية المطاف فاتورة الإصلاح التي ترتب على سوني دفعها جراء الهجوم بما يفوق المليار دولار ناتجة عن ضياع العمليات التجارية والاستشارات الخارجية ومختلف الدعاوى القانونية.

وبعد ذلك، في عام 2014، اعترفت متاجر تارغيت في أنحاء الولايات المتحدة بأنها وقعت ضحية هجوم سايبري استهدف صرافات البطاقات الائتمانية في نقاط البيع لديها. وجاءت هذه الحادثة في أسوأ توقيت بالنسبة لسلسلة التجزئة في ذروة موسم تسوق أعياد الميلاد. فقد تمت في تلك الحادثة سرقة بيانات أكثر من 110 ملايين حساب، في هجوم كان من الواضح أن العقل المدبر الذي يقف وراءه هو قرصان في السابعة عشرة من عمره في روسيا.

فكر بمدى هذه الخسائر الفادحة. لقد تم نشل ثلث الشعب الأميركي تقريباً على حين غرة. لم يسبق في تاريخ البشرية أن أمكن لأي شخص أن يسرق 110 ملايين شيء، ناهيك بنهب 100 مليون شخص دفعة واحدة.

على الرغم من حجم عملية تارغيت ومداها، لم يمر عام واحد حتى تم

تجاوز هذا الرقم من قبل مجموعة قراصنة روس جمعت 1.2 مليار اسم مستخدم مع كلمات مرورهم وغيرها من البيانات السرية من 420.000 موقع إنترنت، وفقاً لتقرير لشركة هولد للأمن. لقد دخلت الجريمة بدورها عصر قانون مور وآثاره الأسّية التي ستطالنا جميعاً.

سيطر على الشيفرة، سيطر على العالم

التقدم التقاني أشبه بفأس في يد مجرم مريض.

ألبرت آينشتاين

إن تعجّل الجنس البشري نحو تحقيق اتصال كلي بالإنترنت يحدث تحولاً في أنفسنا وفي العالم المحيط بنا. ومن هذه التواصلية العالمية سيأتي خير هائل، فسيتحقق العلم الشامل حين تصبح كل حقيقة أو فكرة تم تسجيلها على الإطلاق متوفرة بالزمن الحقيقي، بغض النظر عن مصدرها أو مكانها. من المعادلة الكيميائية للتركيب الضوئي، إلى درجة الحرارة الحالية في باكو، إلى الفريق الفائز في دوري الكريكيت الوطني الإنكليزي عام 1901، وآخر حماقات جستن بيبر، سيصبح من الممكن معرفة أي شيء مع ربطنا أنفسنا بالدماغ العالمي الذي تمثله الإنترنت.

لا تنفك قدرة الإنسان تزداد مع دخول المزيد من أغراض العالم إلى الإنترنت. فيمكنك اليوم تفعيل مشغل الفيديو الرقمي وأنت على الطريق السريع، وتشغيل السيارة من غرفة المعيشة. وتستطيع الطابعات الثلاثية الأبعاد إخراج قطع السيارات والملابس وموادّ البناء. بينما مضخات الأنسولين وأجهزة النبض وأجهزة ضبط الرعشان القلبي المزروعة، تتصل بالإنترنت وتنقل إلى طبيبك بالزمن الحقيقي بيانات قد تنقذ حياتك. بل إن بإمكان الأطباء إجراء عمليات جراحية عابرة للأطلسي بواسطة الروبوتات الجراحية الوكيلة، ليصل الجراحون إلى قرىً لم يسبق لأحد أن زارها من قبل. وبإمكان البشر اليوم أن يتحكموا بأشياء على الطرف الآخر من

الكوكب بطرق كانت في ما مضى ستعتبر مستحيلة لا يمكن تخيلها.

ربما كانت ثمة منافع واضحة من حيث الكلفة والفعالية والإمكانيات المتاحة تقدمها هذه التحولات، لكنها تضيف تعقيداً هائلاً على عالمنا. ولتقدير هذا القدر من التعقيد تقديراً تقريبياً جداً، يمكننا النظر في عدد أسطر التعليمات البرمجية المطلوبة لخلق برمجية معينة أو وظيفة جديدة في نظام معلوماتي. ففي عام 1969 على سبيل المثال، كان الحاسب الملاحي في أبولو 11 الذي قاد رواد الفضاء بأمان عبر مسافة الـ 356,000 كيلومتر التي قطعوها من الأرض إلى القمر وبالعكس، لا يحتوي سوى على 145,000 سطر برمجي، وهو مجموع ضئيل للغاية وإنجاز بارز بمعايير اليوم. ففي بداية الثمانينيات، حين بدأت عمليات المكوك الفضائي، كانت برمجيات الطيران الرئيسية فيها قد وصلت إلى 400,000 سطر.

للمقارنة، تطلبت حزمة أوفيس من مايكروسوفت عام 2013، 45 مليون سطر، بينما تطلب تشغيل مصادم هادرون الكبير للجزيئات في المنظمة الأوروبية للأبحاث النووية قرابة 50 مليون سطر. وتتطلب البرمجيات اللازمة لتشغيل مؤقتات سيارة اعتيادية اليوم 100 مليون سطر برمجي، وهو قدر أقل بكثير من الـ 500 مليون سطر غير المسبوقة، التي تطلبها موقع الويب الخاص ببرنامج هيلثكير الأميركي المثير للجدل. وعلى الرغم من صعوبة إجراء مقارنات مباشرة، يمكن القول إن موقع هيلثكير أكثر تعقيداً بحوالى 35 مرة من نظام الملاحة الذي أوصل أبولو 11 إلى القمر وعاد بها. فهل من عجب في أن الموقع قد انهار واحترق؟

سيكون للتعقيد المتنامي للبرمجيات الحاسوبية مضاعفات مباشرة على الأمن والسلامة العالميين، وخصوصاً مع تحول الأغراض المادية التي نعتمد عليها، كالسيارات والطائرات والجسور والأنفاق والأجهزة الطبية المزروعة، إلى شيفرات حاسوبية. والأشياء تتحول أكثر فأكثر إلى تقانة المعلومات.

فالسيارات هي "حواسب نستقلها"، ولم تعد الطائرات سوى "نظم تشغيل سولاريس تطير متصلة بصناديق أنظمة التحكم الصناعية". ومع ازدياد حجم هذه الشيفرات البرمجية وتعقيدها، يزداد أيضاً عدد الأخطاء والثغرات البرمجية. فوفقاً لدراسة أعدتها جامعة كارنيجي ميلون، تحتوي كل برمجية على عشرين إلى ثلاثين ثغرة لكل ألف سطر تعليمات برمجية في المتوسط، أي إن الخمسين مليون سطر تحتوي على مليون إلى مليون ونصف المليون خطأ يمكن استغلاله. وهذا هو أساس أي هجوم تنفذه برمجيات خبيثة، فهي تستغل هذه الثغرات الحاسوبية بحيث تجعل الشيفرة البرمجية تنفذ شيئاً آخر غير ما كانت معدة لتنفيذه. ومع الاستفاضة في كتابة التعليمات البرمجية، تتكاثر الثغرات ويتراجع الأمن، وتزداد العواقب التي تحيق بالمجتمع ككل.

من شأن التعقيد المتزايد للأنظمة أن يشكل مصدر خطر كبير، حتى حين لا يستغله الأشرار. ولنأخذ هنا مثالاً في الانقطاع الكهربائي الذي وقع في الشمال الشرقي عام 2003، تاركاً خمسة وخمسين مليون شخص في كندا والولايات المتحدة يتخبطون في العتمة لعدة أيام. فقد أدت متاهة من الكابلات الكهربائية وخطأ تشغيلي، إضافة إلى ثغرة برمجية، إلى أكبر انقطاع كهربائي في تاريخ أميركا الشمالي. كما أدّت أخطاء الحاسب دوراً في كارثة منصة التنقيب عن النفط ديبووتر هورايزن، التي قضت على حياة أحد عشر عاملاً، وأدت إلى أكبر كارثة بيئية في التاريخ الأميركي، حين تسرب 4.9 ملايين برميل نفط في خليج مكسيكو. فخلال جلسة الاستماع الحكومية حول الكارثة، شهد ميشيل ويليامز، كبير التقنيين الكهربائيين على متن المنصة، بأن النظم الأساسية لمراقبة الحفر والتحكم به كانت مشلولة نتيجة الانهيارات البرمجية المتتالية، التي انتهت بظهور "شاشة الموت الزرقاء" على حاسب الحفارة قبيل الانفجار الذي أدى إلى غرق المنصة.

وعلى الرغم من أن انقطاع الكهرباء في الشمال الشرقي عام 2003، وكارثة منصة ديبووتر هورايزن كان كلاهما حادثاً بجميع المقاييس، فإنهما يقدمان لنا تصوراً عن الضرر الهائل الذي قد ينشأ عن أخطاء النظم الحاسوبية. إلا أن فشل النظام الحاسوبي نتيجة حادث أم نتيجة عمل إجرامي ليس سوى مسألة نوايا. فإذا أخذنا العدد الضخم من الثغرات الموجودة في شيفرات الحواسب الحديثة بالاعتبار، فكيف ستكون النتيجة إذا ما توفرت النوايا الشريرة أيضاً؟ إن التقانة نفسها القادرة على إنقاذ العالم وتمكين العولمة، قد يستغلها المتطرفون والمجرمون والإرهابيون والحكومات لتدميره.

لسوء الحظ، بعد أن يخرج سلاح سايبري إلى الملأ فإنه لن يعود ويختفي، بل يصبح بالإمكان إعادة توجيهه. فخلافاً للقنابل التقليدية، والتي تنفجر متحولة إلى ملايين الشظايا حين تسقط على أهدافها، يمكن إعادة استخدام البرمجيات الخبيثة مرة بعد أخرى. وإذا كان بإمكان مسؤولي الجيش والاستخبارات إنفاق الملايين من الدولارات سراً على تطوير سلاح معين، فإن الشيفرة البرمجية سهلة النسخ. وما إن تصدر حتى تصبح متاحة للناشطين السايبريين والعصابات الإجرامية والإرهابيين، يمكنهم استغلالها لأهدافهم الخاصة، ما يقود إلى أشكال جديدة من انتشار الأسلحة السايبرية.

يمكنك تخيل الأمر كزجاجة مولوتوف افتراضية إذا ما رُميت على هدفها أمكن رميها من جديد حيث أتت. وقد سبق لنا أن رأينا ذلك يحدث حين قامت المنظمات الإجرامية والحكومات المارقة بنسخ تصاميم كانت تستخدم في الأصل ضدها، فكانت تعيد توجيهها لتنفذ هجمات خاصة بها. ومع استمرار تحويل الشيفرات الحاسوبية إلى أسلحة، ستصبح هجومات كهذه أكثر شيوعاً وأكثر تعقيداً في آن معاً.

من المقلق، لكنها الحقيقة، أنه لم يتم حتى اليوم خلق أي نظام حاسوبي غير قابل للاختراق، إنها حقيقة مقنطة إذا ما نظرنا إلى اعتمادنا الشامل على

هذه الآلات في كل شيء، من الاتصالات إلى النقل والرعاية الصحية. فليست كلمات المرور وفحوصات النظام هي وحدها التي جعلت ماتّ هونان في غاية الضعف، بل المسألة متعلقة بجميع البرمجيات التي نستخدمها لتسيير العالم. من المؤلم القول إنه حين يكون كل شيء متصلاً، يكون الجميع في حالة ضعف.

لا تنطبق طاقة قانون مور على الجوانب الإيجابية من التقانة فقط، بل على تلك السلبية أيضاً. ومع قانون مور تأتي أيضاً الجريمة الخاضعة لقانون مور، أي المجرمين والإرهابيين والناشطين السايبريين وممثلي الدول الذين يستغلون التقانة بدورهم. وهم على علم تام بكيفية استغلال تعقيدات النظام والبرمجيات الرديئة، لانتزاع ما يريدونه من حضارتنا القائمة على التقانة السريعة التطور. ومع تحول جميع الأشياء إلى حواسب، ولكون الأخيرة تعمل بالشيفرات البرمجية، فإن هذه الأطراف الجديدة الخارجة عن القانون تدرك بوضوح أن من يحكم قبضته على الشيفرة يحكم قبضته على العالم. لكن ليس المجرمون والحكومات المارقة هم وحدهم من علينا أن نحذر. فغالباً ما تكون الشركات والمنظمات التي نعتمد عليها في الحماية والمشورة والترفيه هي تحديداً من يجعلنا ضعفاء على نحو لا يعقل، فهي تسيطر بدورها على الشيفرات التي تسيّر حياتنا.

الفصل الرابع

أنت لست الزبون، بل السلعة

ستمنحك الحقيقة الحريّة، ولكنها ستزعجك أولاً.

غلوريا ستينيم

داء باركينسون، التصلب اللويحي الناكس المتعاود، التهاب اللفافة المنخر، ابيضاض الدم اللمفاوي الحاد، السكري الشبابي، الإيدز، التصلب الجانبي الضموري. إن تشخيص أيّ من هذه الأمراض كفيل بلا شك بدبّ الرعب في قلب أي مريض، إذا ما تلقى مثل هذا الأخبار التي ستغير مجرى حياته. في السنوات الماضية، كان المصابون بمثل هذه الأمراض يجدون أنفسهم مكتئبين ووحيدين وعاجزين عن مناقشة حالتهم مع الآخرين، الذين يعرفون تماماً الحالة التي يمرون بها. علاوةً على ذلك، سوف تسهم نُدرة المعلومات الطبية المفهومة بالنسبة للبشر في عزلة هؤلاء المرضى عن أصدقائهم وعائلاتهم.

لهذا السبب أسس جيمي وبين هيوود (وكان أخوهما مصاباً بمرض لو غيريغ) موقع PatientsLikeMe.com، ليسمحا لزوار الموقع بمشاركة قصصهم والتواصل مع غيرهم ممن لديهم التجارب والمِحن الصحيّة نفسها. ومنذ نشأة الموقع عام 2004، توسع ليصبح مجتمعاً عالمياً يضم أكثر من 200,0 مريض يعانون ألفاً وخمسمئة مرض نادر. وأصبح الموقع بمثابة المنقذ الرمزي والموضوعي بالنسبة لآلاف الأشخاص، حيث كان المرضى يزدادون معرفة بمرضهم ويتبادلون الطرق وسجلاّت المعالجات السابقة، التي تبقيهم على قيد الحياة من خلال عدد من منتديات النقاش على الموقع نفسه.

كانت فرصة التواصل مع الآخرين على هذا النحو هي أول ما جذب بلال أحمد إلى الموقع، وهو رجل أعمال عمره ثلاثة وثلاثون عاماً من مدينة سيدني في أستراليا. كان أحمد يعاني القلق والاكتئاب منذ وفاة والدته، وكان

يجد صعوبة في مناقشة حالته مع الأصدقاء والعائلة.

أنشأ أحمد حساباً باسم مستعار على الموقع، وانضم إلى المنتدى المتخصص بموضوع المزاج، الذي يتبادل فيه المستخدمون التفاصيل الأساسية للاضطرابات العاطفية مثل الاضطراب الثنائي القطب ومتلازمة ما بعد الرض وفقدان الشهية العصابي والوسواس القهري ونوايا الانتحار. في منتدى المزاج، وضع أحمد طوعاً، قائمة تتضمن أعراض مرضه ونتائج فحوصاته وجميع الأدوية التي وُصِفت له لعلاج الاكتئاب. وكان أحمد يتواصل في هذا المنتدى مع مرضى آخرين حول العالم ويقيم معهم علاقات الصداقة ويشاركهم التفاصيل الأساسية حول مرضه على موقع محمي بكلمة مرور، وكان يتلقى بدوره الدعم الذي كان يصبو إليه.

لهذا السبب شعر أحمد بتعرضه لانتهاك كبير حين أخبره الموقع عن "نشاطٍ غير قانوني" في مجالس النقاشات، التي تدور في منتدى المزاج. ففي الساعة الواحدة صباحاً من السابع من أيار عام 2010، لاحظ مديرو النظام نشاطاً مشبوهاً مصدره العديد من الحسابات الجديدة التي كانت تمارس "الجزّ"، أي كانت تنسخ كل رسالة موجودة على المنتدى الخاص، ثم تنزل المعلومات على موقع آخر. تمكن الموقع في النهاية من تحديد هوية الدخيل المسؤول عن هذا الاختراق، والذي لم يكن سوى شركة نيلسن، المارد الإعلاني نفسه المشهور بتقييمات نيلسن لمحطات التلفزة. وقد اعترفت شركة مكلفة من قبل نيلسن ومعروفة باسم بازميتريكس بأخذها البيانات، حيث أضافتها إلى مجموعة المعلومات التي لديها والمسروقة من 130 مليون مدونة أخرى وثمانية آلاف منتدى، إضافة إلى تويتر وفايسبوك، وغيرها من مواقع الشبكات الاجتماعية التي كانت تتعقبها. كانت شركة نيلسن تبيع هذه البيانات إلى المعلنين والتجار، وفي هذه الحالة، المؤسسات الدوائية الرئيسية كموادّ خام في إطار صناعة استثمار البيانات العالمية، التي تدر

أرباحاً تقدر بمليارات الدولارات.

مع أن هذا النشاط الفاضح لشركة نيلسن يعتبر مجافياً للأخلاق، إلا أنه قانوني من الناحية التقنية وفقاً للقانون الفدرالي الحالي. في 18 أيار عام 20، كشف الموقع عن الحادثة لكافة مستخدميه. كما انتهزت الشركة الفرصة لتذكر المستخدمين بمعايير سياسة الخصوصية لديها وشروطها:

> نأخذ المعلومات التي يقدمها المرضى ويتشاركونها في ما يخص تجاربهم مع الأمراض ونبيعها لشركائنا (أي الشركات التي تطور وتبيع المنتجات للمرضى). هذه المنتجات قد تتضمن الأدوية والأجهزة والمعدات والتأمين والخدمات الطبية... وعليكم أن تتوقعوا أن كل معلومة تقدمونها (حتى لو أنها لم تعرض حالياً) قد تتم مشاركتها.

مهلاً، ماذا؟ كانت المذكرة التي فضحت اختراق نيلسن سيئة بما فيه الكفاية، لكن البريد الإلكتروني الذي تبع ذلك ووضح تفاصيل السياسة الخاصة للموقع كان صرخة إيقاظ قوية. كانت هذه بالنسبة لمعظم مستخدمي الموقع هي المرة الأولى التي يُدركون فيها أن جميع المعلومات الطبية التي كانت في الماضي ستبقى محفوظة بأمان في خزانات عيادات أطبائهم، هذه المعلومات التي تشمل حالاتهم وتواريخ التشخيص الخاصة بهم وتاريخ عائلاتهم وأعراض مرضهم، وقياسات بروتينات التمايز والمقادير الفيروسية والنتائج المخبرية والمعلومات الشخصية والجنس والعمر والصور بل وسلاسلهم الجينية برمتها، أصبحت الآن تُباع من قبل موقع Pa، هذا المكان الذي كان محل ثقة بالنسبة لهؤلاء المرضى المكتئبين على أمل أن يساعدهم ويصون معلوماتهم.

مع أن موقع PatientsLikeMe.com زعم أنه لم يبع سوى بياناتٍ محايدة مجهولة الهوية عن مرضاه، فإن هناك شركات بيانات جديدة بارزة

مثل شركة بيك يو المحدودة المسؤولية في نيويورك، تعمل منذ وقت طويل على استنباط تقنيات متنوعة يمكن حمايتها ببراءة اختراع تقوم بالربط بين الأسماء الحقيقية للناس وبين تلك المزيفة التي يستخدمونها في المذكرات وغرف المحادثة وعلى تويتر. بمعنى آخر، لن يكون على أي شركة دوائية أو شركة تأمين صحي تريد معلومات من موقع PatientsLikeMe.com سوى طلب خدمات بيك يو لتطبيق هندسة عكسية على اسم المستخدم الخاص بك أو اسمك المستعار لتحديد هويتك بالكامل. ففي حالة بلال أحمد، يعني ذلك أن جميع البيانات الشخصية التي وضعها في عهدة موقع Pa أصبحت الآن بيد نيلسن/باز ميتريكس. وقد أشار أحمد في مقابلة علنية أجريت بعد الكشف عن هويته، إلى أنه شعر بإهانة كبيرة بسبب الحادثة وسارع إلى حذف كافة الكتابات التي وضعها على الموقع بالإضافة إلى قائمة الأدوية التي كانت قد وُصِفَت له، لكن بالطبع كان قد فات الأوان على ذلك. ففي كل مرةٍ كان أحمد وغيره من المرضى يبنون على موقع P حسابات مفصلة عن أمراضهم وأعراضها، كانت هناك شركات متوارية مثل نيلسن تجمع كافة البيانات التي تمت مشاركتها مع الآخرين. أما بقية البيانات التي لا تتم سرقتها من أطراف أخرى فإنها تُباع لدى موقع Pat نفسه، الأمر الذي تكشفه سياسة الخصوصية المطبوعة بتأنق في الموقع، والتي لم يفلح أحمد وبقية المرضى في قراءتها ولو مرة واحدة عندما أنشأوا حساباتهم.

كما كان على أحمد أن يكتشف في ما بعد، فإن الشبكات الاجتماعية هي السجلات العامة الجديدة. فكل ما تُشاركُه، بقصدٍ أو بغير قصد، يتم تجميعه وفرزه وتخزينه من قبل شركاتٍ ضخمة عالمية جديدة ثم يتم بيعه للمعلنين والحكومات وغيرهم من سماسرة البيانات، وجميعهم يتمتع بشَرَه كبير لمعرفة أدق التفاصيل عن حياتك. ويُمكن استخدام هذه البيانات

لتحديد ما إذا كانت لديك مسبقاً ظروف صحية معينة أو كان عليك أن تدفع مبالغ أكبر مقابل التأمين على حياتك، أو كنت غير مؤهل لعمل أو لترقية في وظيفتك. وإذا كانت المشاركة تعني الاهتمام، فهي قد تعني أيضاً مبالغ عالية للتأمين. وفي النهاية، تعلم مئات الآلاف ممن يستخدمون موقع F درساً قيماً، وإن كان مؤلماً، هو أنهم في الحقيقة لم يكونوا زبائن الموقع، بل سلعاً تُباع إلى أعلى المزايدين في محاولة لتحقيق الأهداف التجارية للشركة.

عالمنا الرقمي المتنامي، ما لم يسبق لأحد أن أخبرك به

في بداية عام 2013، كان الأميركيون يقضون أكثر من خمس ساعات يومياً على الإنترنت عبر أجهزتهم الرقمية. فنحن نطالع الأخبار من خلال مواقع مثل سي.إن.إن ونيويورك تايمز وإي.إس.بي.إن، ونتحقق من أرصدتنا البنكية من خلال مواقع سيتي بانك وويلز فارغو. نتسوق على موقعي أمازون وماسيز. وندفع فواتير كونإد وكومكاست، ونرتب مواعيدنا مع أطبائنا ونتحقق من التأمين الصحي عن طريق البلو كروس. نشاهد مسلسل بيت من ورق على موقع نيتفليكس ومسلسل داونتاون أبي على موقع هولو. وما هذه سوى بداية. لنتأمل ولو للحظة كيف نستخدم هواتفنا الذكية كل يوم، فثمانون بالمئة منا يتحققون من الرسائل على هواتفهم خلال أول ربع ساعة بعد الاستيقاظ من النوم. هل أعطيت أصدقاءك تحديث حالة سريعاً على الفايسبوك اليوم؟ على الأرجح أنك ستتلقى "إعجاباً" أو اثنين، أو ربما تعليقاً دمثاً من أحد أصدقائك. وماذا عن الصور الشخصية التي التقطتها لنفسكِ وأرسلتها لصديقكِ؟ لقد أصبحت الإنترنت مكنزاً واسعاً ومجانياً مليئاً بالمعلومات وموادّ الترفيه، لكننا بذلك نسلم رقابنا طواعية. ففي كل خطوة نقوم بها نخلف وراءنا أثراً رقمياً كبيراً يكفي لملء مكتبة الكونغرس عدة مراتٍ يومياً. أما كيف نشأت هذه البيانات وخُزّنت وحُللت وبيعت، فهذه كلها تفاصيل يتغاضى معظمنا عنها بسرور معرّضين أنفسهم للخطر.

لا يمكن إنكار سُلطة الوسائط الاجتماعية. ففي غضون عشرة أعوام فقط انقضت على نشأته عام 2004، استطاع الفايسبوك الارتقاء وبسرعة من لا شيء إلى 1.3 مليارات عضو من كافة أنحاء العالم. وفي كل يوم يتم رفع 350 مليون صورة، فيما يتم ضغط زر الإعجاب الحاضر في كل مكان 6 مليارات مرة. توثق الوسائط الاجتماعية مواعيدنا الغرامية، وحفلات تخرجنا في الجامعات، والمنازل التي نشتريها والولادات والأطفال الجدد والزيجات والطلاق. لكنها قد تكون أيضاً وسائل للتغيير الجيوسياسي، كما كان واضحاً من خلال الربيع العربي سنة 2010 عندما قام مدير في غوغل، واسمه وائل غنيم، بإنشاء صفحة على الفايسبوك ليلقي الضوء على مقتل شاب مصري متظاهر على أيدي قوات الأمن التابعة لحسني مبارك. "بعد دقيقتين فقط من انطلاق صفحته على الفايسبوك، انضم إليها 300 شخص". تضاعف الرقم بعد ثلاثة أشهر ليصبح 250,000 شخص. وعلى نحو مماثل نُسبَت إلى تويتر وغوغل وغيرها من الخدمات المساعدة في قيادة التغيير في تونس وإيران وليبيا. وربما يبقى على التاريخ أن يحكم على الدور الذي أدته الوسائط الاجتماعية في الربيع العربي، لكن لا شك في أن هذه الخدمات قد تكون قوة لعمل الخير.

جاذبية هذه الوسائل واضحة. ففي النهاية، يقضي معظمنا حياته في التجول عبر الإنترنت بحثاً عن الموسيقى ووصفات الطعام ونصائح الاستثمار والأخبار والإرشادات وفرص العمل وإشاعات المشاهير ونتائج المباريات الرياضية. وعندما لا نتحقق من بريدنا الإلكتروني، تجدنا نلعب ألعاباً مثل تيمبل ران أو فروت نينجا، وهي كلها مجانية التحميل. فحتى الرسوم التي كنا ندفعها لوكلاء السفر والصحف وشركات الموسيقى، كلها اختفت وألغيت، ويعود الفضل في ذلك إلى الأشخاص الأسخياء الذين قدموا لنا الشبكة العنكبوتية العالمية. لكن هل خطر ببالك يوماً أن تتساءل لماذا لا

يرسل لك غوغل فاتورةً؟

اسأل شخصاً عادياً لماذا تتوفر خدمات غوغل وفايسبوك وتويتر ويوتيوب ولينكيدإن مجّاناً، وستجد أنه سيرتبك حين يدخل في التفاصيل. إذ يعتقد الكثيرون أن تمويل كل ذلك يتم عن طريق الإعلان، والمقصود هنا تلك اللوحات الإعلانية المزعجة أو الشاشات المنبثقة التي لا تنفك تظهر أمام وجهنا. ربما كان ذلك بالفعل هو السبب، لكنه ليس سوى جزء صغير من القصة. وقد يظن البعض الآخر أن المسألة مرتبطة بمصلحة متبادلة بسيطة للغاية. فهذه الشركات تعطينا خدمات مجانية قيّمة، مثل البريد الإلكتروني والأخبار والفيديوهات ومساحات التخزين لنضع فيها الصور، بينما نقوم نحن بدورنا بإعطائها قدراً ضئيلاً من المعلومات عن أنفسنا. فنحن بحاجةٍ من حين إلى آخر إلى مشاهدة إعلان صُمّم خصيصاً ليتناسب مع حاجاتنا، لكن إعدادات الخصوصية المتاحة لنا كفيلة بتسليمنا زمام الأمور وما من أحد يتأذى، أليس كذلك؟ ليت الأمر كان بهذه البساطة. فحقيقة الصفقة التي قمنا بها مقلقة للغاية.

لنأخذ غوغل على سبيل المثال، وهي شركة أسسها عام 1998 طالبا دكتوراه في جامعة ستانفورد، وهما لاري بيج وسيرجي برين. ففي ورشة عمل مشتركة في مينلو بارك في كاليفورنيا، اخترع الاثنان خوارزمية ثورية جديدة حققت تحسيناً كبيراً لنتائج البحث على الشبكة العنكبوتية العالمية الحديثة، جاذبين بذلك العديد من المعجبين المخلصين بفضل بساطة الواجهة الرسومية والجودة العالية التي أمكن تحقيقها لنتائج البحث. وفي عام 2000، بدأ كل منهما ببيع كلمات مفتاحية لمنتجات معينة تتناسب مع أي عبارة توضع للبحث. فمثلاً، إذا كان سؤالك عن "باريس، فرنسا"، فستجد روابط تشير إلى الخطوط الجوية الفرنسية وشركات تأمين السفر أو حتى مجموعة فنادق هيلتون. وصار بإمكان الشركات الباحثة عن زبائن

جدد الآن التسويق عن طريق إعلانات الكلمات المفتاحية على غوغل مع دقة غير مسبوقة، للحصول على عائدات أفضل لدولارات الإعلان التي تنفقها. إذاً، ما بدأ كفكرة متواضعة من طالبين في ستانفورد في عام 1998، نمى ليتحول بحلول سنة 2015 إلى قوة عالمية هائلة.

ومع مرور السنين، قدم غوغل عدداً كبيراً من المنتجات التي تجعل حياتنا أبسط وأكثر إنتاجية. عندما أطلق غوغل خدمة جيميل عام 2004، قدم مساحة تخزين بيانات مذهلة بحجم واحد غيغابايت، فاقت بكثير الحجم التافه البالغ 2 ميغابايت، الذي كان يقدمه اللاعب المهيمن على الساحة موقع هوتميل التابع لمايكروسوفت. وبينما كانت الشركة الشابة تشق طريقها، ظهرت منتجات رائعة أخرى قُدمت لنا، مثل تقويم غوغل كاليندر وغوغل كونتاكتس لإدارة العناوين وخرائط غوغل مابس وأطلس غوغل إيرث وغوغل فويس للاتصال الصوتي، وغوغل دوكس لإدارة المستندات وغوغل ستريت فيو وغوغل ترانسليت وغوغل درايف وغوغل فوتوز (بيكاسا)، وغوغل فيديو (يوتيوب) وغوغل كروم وغوغل+ وغوغل أندرويد، والقائمة تطول. خدمة تلو الأخرى، باتت خدمات مثل المكالمات الهاتفية والترجمة والخرائط ومعالجة النصوص، هذه الخدمات التي كنا في السابق ندفع مئات الدولارات للحصول عليها (إذا ما فكرنا بمايكروسوفت أوفيس)، أصبحت الآن فجأة مجانية.

أفضل تفسير حسن النية لهذا السخاء هو أن غوغل كان فقط يقدم المنتجات التي يحتاج إليها العامة، والتي ترضي حاجاتنا التكنولوجية المتزايدة (وأيضاً حاجات المعلنين). ربما كان هناك تفسير أقل سخاءً، هو أن يكون كل واحد من تلك المنتجات المذكورة آنفاً أُنشئَ بقصدٍ معين، ليخدع ويداهن ويفتن المستخدمين لكي يكشفوا إلى الأبد عن مقدارٍ متزايد من البيانات الخاصة بهم وبحياتهم. قد يذهل الناس إذا ما فهموا الطبيعة

الحقيقية لهذه الصفقة. حسناً، لنعد صياغة أوتو فون بيسمارك: الأفضل لزبائن غوغل ألا يروا أو يعرفوا تماماً كيف تمت صناعة النقانق. لكن سحب الستار لدراسة معمل النقانق هو الأساس في فهم المخاطر الأمنية الكبيرة المرتبطة بالبيانات التي تواجه عالمنا اليوم.

بدأ الاختلاس التدريجي للبيانات وبشكلٍ بريء بما فيه الكفاية، عندما قمتَ لأول مرة باستخدام الغوغل للبحث في شبكة الويب. فبينما تبحث، يقوم غوغل بتتبع العملية وتسجيل كافة كلمات البحث، ناهيك بتسجيل كل رابط تضغط عليه. من ذلك المنتج الأولي للبحث، يتم الاكتساب المنسق بعناية لمعلوماتك الشخصية وبدقةٍ بارعة. لكن في النهاية، لم يكن محرك البحث هذا كافياً، لذلك قامت غوغل بالتماس طرقٍ إضافية للولوج على نحو أعمق إلى داخلك، إلى آمالك وأحلامك ورغباتك. وكانت النتيجة هي بريد جيميل الإلكتروني. فبتقديمه مقداراً كبيراً من مساحة التخزين وتجربة استخدام في غاية السلاسة، استطاعت غوغل أن تصل إلى كل بريدك الإلكتروني الشخصي والمهني. فقد أصبح غوغل الآن قادراً على فهم كل شيء تكتبه ويعلم إلى من ترسله، ولم يعد يكتفي بعمليات البحث الذي تقوم بها. كان غوغل يقوم بمسح وقراءة رسائلك إلكترونياً ليعثر على مفاهيم جديدة يمكن أن تُقدم للمعلنين، ليرفع رسومه باستمرار كلما قام بصقل الملف الذي يحتفظ به عنك. إذا كتبت رسالة لوالدتك تخبرها فيها أنك حزين بسبب انهيار عصبي تعرضت له مؤخراً، فإن غوغل قد يقترح عليك مضاداً للاكتئاب أو نادياً للمرح أو عطلة في جزر الكاريبي. وطالما بقيت على اتصال على الجيميل، فإن بإمكانه اقتفاء أثر كافة عمليات البحث التي تقوم بها وربطها برقم تعريفك الخاص لديه. وبالنتيجة، يصبح ملفك لدى غوغل أغنى، وكذا تصبح الشركة نفسها.

عندما يقدم لك غوغل فرصة حفظ اتصالاتك على الشبكة، يقوم بدوره

بتقييم حجم شبكتك الاجتماعية وشدة ترابطها وقوتها الشرائية. وعندما يقدم غوغل برامج الخرائط الخاصة به ويزودك مجاناً بنظام تحديد المواقع وإرشادات القيادة، فإن بإمكانه الآن تتبع الأمكنة التي تذهب إليها. يتساءل الغوغل عن الأشخاص الذين تتواصل معهم، ولذلك أحدث غوغل فويس ليعرف الحقيقة. فصار بإمكانه الآن لا فقط تتبع كل مكالمة هاتفية تقوم بها، بل تسجيل رسائلك الصوتية باستخدام برمجيات تعرّف الصوت وتسجيله. كان ذلك عملاً تقنياً ممتازاً في ذلك الوقت، يسمح لغوغل أيضاً بأن يفهم النقاش الذي كان يدور بينك وبين من يحاورك. فإذا ترك لك شخص ما رسالة صوتية يقترح فيها عليك طعاماً إيطالياً لأجل العشاء، سيقوم غوغل ببيع هذه المعلومة للمعلنين لتظهر لك فجأة إعلانات للبيتزا في أنحاء عالم غوغل الخاص بك. وتوخياً لمزيد من الدقة، أنشأ غوغل نظام تشغيل أندرويد وقدمه مجاناً. بالمقابل، يستطيع الغوغل الآن أن يقتفي أثرك أينما ذهبت وأخذت معك هاتفك الذكي.

بالطبع لو أخبرك غوغل بكل هذه الأمور لفقدت صوابك، لكنه بدلاً من ذلك اخترع خدعة ظريفة أشبه بورقة التين. فعندما اختُرِع غوغل، صوّر نفسه على أنه الضحية المظلومة وأنه الشخص الذي يقاتل مايكروسوفت الشرير. أراد غوغل أن يخبر مستخدميه أنه يهدف للخير، ولهذا قرر جعل عبارة "لا تكن شريراً" شعاراً رسمياً لشركته. ولكي يخفف من الشكوك الدائمة، أنشأ غوغل أيقوناته ورسومه، مثل الشعار البريء المتعدد الألوان وصبي الأندرويد البديع الأخضر، لتكون فاتنة ومسالمة وبالتالي يمكن الوثوق بها. رسوم غوغل العبثية ولوحاته التي تحتفل بالجميع، بدءاً بمارتن لوثر كينغ وحتى غاندي، تجعل بدورها العامة يطمئنون بأنهم يتعاملون مع الأخيار. إضافة إلى ذلك، لدى غوغل كل سياسات الخصوصية التي ستؤمن لي الحماية، أليس كذلك؟ لا تتعجل!

بالنظر للأمر ببعض الريبة، لم يطور غوغل منتجاته فقط ليعطيك البريد المجاني، بل لكي يحصل منك على البيانات. فكما تاجر المخدرات الذي يناول أول كيس من الهيروين لذلك الشخص الذي سيصبح قريباً مدمن مخدرات، قدم لك غوغل شيئاً "على حساب المحل"، وسيمر بعض الوقت إلى أن تدرك المعاني الضمنية للصفقة التي قمت بها، ولكن بعد فوات الأوان. وقد أصبح الأمر جلياً عندما أعلن غوغل في بداية عام 2012 أنه يقوم بدمج بياناته عبر كافة منتجاته، البالغ عددها سبعين منتجاً وخدمةً. والنتيجة هي رؤية موحدة وعميقة غير مسبوقة لك ولعالمك. ففي السابق، كانت عمليات بحثك على غوغل وما تقوم به على هاتفك الذكي، والفيديوهات التي تشاهدها على يوتيوب عبارة عن بيانات يقوم غوغل نظرياً باحتوائها كلٍّ على حدة. لكن ليس بعد الآن، فقد أصبحت لدى غوغل صورة موحدة ومفصلة عنك وعن كل ما تقوم به من خلال منظومته. حتى إن كثيرين يحاجون بأن غوغل يعرفك أكثر مما تعرف نفسك. فامتلاكه كلّ هذه البيانات هو تحديداً ما يمكّنه من طلب مبالغ كبيرة من المعلنين مقابل معلوماتك.

إذا لم يكن الأمر واضحاً في السابق، فإنك لست زبون غوغل بل سلعته، وهذا هو السبب وراء عدم حصولك على فاتورة. ولهذا السبب أيضاً ليس هناك رقم 800 للدعم التقني. فقد تم ادّخار مثل هذه الخدمات لأجل زبائنه الحقيقيين، أي المعلنين الذين يشترون كل البيانات التي قمت بنشرها على طريق المعلومات السريع التي يوفرها غوغل. أنت الشيء الذي يبيعه غوغل للآخرين؛ وهذه هي الصفقة التي لم يشرحها لك غوغل يوماً. وسواء أدركت ذلك أم لا، فإنك مسهم كلياً في ذلك.

يزيد غوغل على رصيده منتجاتٍ رائعة تلبي احتياجات مستخدميه، فالشركة تعجّ بأعدادٍ كبيرة من الموظفين الأذكياء والمتفانين في عملهم. لكن

لا تُخطئ، إذ سيبقى ولاؤه في المقام الأول لمعلنيه الذين يدفعون الفواتير، وللمسهمين الذين تعهد لهم بالوكالة أن ينتزع منك (بما أنك منتجه والمورد له) أكبر قيمة ممكنة. لهذا السبب يقوم غوغل بتخزين كل بحث قمت به على الإطلاق على الموقع وبشكلٍ غير محدد: "جمهوريّو جامعة الولاية في أوهايو" التي بحثت عنها منذ عشر سنوات، "أعراض مرض السيلان" بعد قضاء ليلة حميمة، "فيديوهات الفتيات المتهورات" التي بحثت عنها في الفندق أثناء سفرك في رحلة عمل، "هل زوجي شاذ؟" التي بحثت عنها سيدة كانت تشعر بالاكتئاب والعزلة.

لا ينسى غوغل ولا يحذف أي شيء، بل يستخدم كلاً من الاستفسارات السابقة، لرسم صورةٍ لك ولتصنيفك وبيعك للمعلنين وجامعي البيانات الذين يقومون بدورهم بوضع افتراضاتٍ عنك، معتمدين على عمليات البحث التي قمت بها وعلى بريدك الإلكتروني، والرسائل الصوتية والصور والفيديوهات والمواقع كما صنفها لهم الغوغل. ربما تتساءل عن حجم البيانات التي يعالجها غوغل يومياً. يصل حجم هذه البيانات إلى حوالى 24 بيتابايت (وهو مقياس يُستخدم لوصف حجم البيانات يعادل مليون غيغابايت أو ألف تيرابايت). لنقرب ذلك من تصورنا، "يكفي غيغابايت واحد لتخزين رف كتب بطول تسعة أمتار" على وجه التقريب. ولو تمت طباعة جميع البيانات التي يعالجها غوغل في اليوم الواحد على شكل كتب ووضعها بعضها فوق بعض، فإن كدسة الكتب الناتجة ستصل إلى منتصف الطريق بين الأرض والقمر. هذا هو حجم المعلومات التي يخزنها لك غوغل، كل يوم!

بوجود جميع هذه البيانات، يبني غوغل تصورات شاملة ويحقق سلطة هائلة، لكن كما يقول القدماء، السلطةُ تُفسِد. فحول العالم، كان غوغل وباستمرار يتعرض للمقاضاة بسبب انتهاكات الخصوصية والخروقات

الأمنية، وسوء استخدام بيانات المستخدمين وسرقة الملكية الفكرية والتملص من الضرائب، ومخالفات قوانين مكافحة الاحتكار. وبعد دعوى قضائية صادرة عن ثمانية وثلاثين مستشاراً قضائياً أميركياً عام 2013، اعترف غوغل بأن سيارات ستريت فيو ذات المظهر الغريب والمزودة بكاميرات عالية التقانة قادرة على الدوران 360 درجة، لا تقوم فقط بالتقاط الصور أثناء مرورها في الشوارع المجاورة لوضعها على خدمة ستريت فيو في نظام خرائط غوغل، بل تقوم أيضاً باختلاس البيانات من الحواسب التي في بيوتنا ومكاتبنا، بما فيها كلمات المرور والبريد الإلكتروني والصور ورسائل المحادثة وغيرها من المعلومات الشخصية من مستخدمي الحواسب الغافلين.

وفي تشرين الأول عام 2013، رفض قاضٍ فدرالي إسقاط دعوى قضائية جماعية ضد غوغل، تدّعي قيامه بقراءة ونسخ حسابات مستخدمي جيميل، منتهكاً بذلك القوانين الأميركية ضد الاعتراض غير القانوني والتنصت على المحادثات. وقبل ذلك، في سنة 2012، تم تغريم غوغل بمبلغ 22.5 مليون دولار من قبل لجنة التجارة الفدرالية، عندما اتضح أن غوغل كان يقوم وبصورة روتينية بالالتفاف على إعدادات الخصوصية على حواسب أبل والحواسب التي تستخدم متصفح سافاري من أبل، ليتتبع المستخدمين عبر الشبكة مخالفاً رغباتهم التي كانوا قد صرحوا بها.

لا شك في أن غوغل شركة مبدعة، وهي في سعيها لنيل المزيد من البيانات حولك لتقدمها لزبائنها الحقيقيين (أي المعلنين)، نجحت في تصميم مجموعة من المنتجات الجديدة التي قد تجعل هواجس الخصوصية السابقة هزيلة بالمقارنة بتلك المستقبلية. وأحد هذه المنتجات هو نظارات غوغل، وهي حاسب قابل للارتداء على شكل نظارات، يُظهر "عرضاً بصرياً مركباً على الرأس". يتصل بالإنترنت وقادر على عرض معلومات بصرية على شاشةٍ مدمجة في الزجاج. ويعمل الجهاز بنظام أندرويد ويمكن له التقاط

الصور والفيديو وبثها في الوقت نفسه بواسطة الكاميرا والميكروفون المدمجين.

في بداية عام 2014، كانت نظارات غوغل موضوع حلقة من مسلسل سيمبسونز بعنوان "نظارة العيون والمدينة". يتم فيها منح كافة موظفي السيد بيرنز زوجاً من "نظارات أوغل". في هذا المشهد، يقوم السيد هومير سيمبسون وزملاؤه باستخدام النظارات لرؤية معلوماتٍ جديدة عن الأشياء والناس من حولهم. وكان نذير الشؤم، أو ربما النبوءة، أن يستطيع السيد بيرنز وهو جالس في مركز التحكم بالمكاتب الوصول إلى كافة نظارات جميع موظفيه ورؤية ما يفعلونه ويشاهدونه بالزمن الحقيقي (في محاولة لتقليل سرقة محتويات المكاتب).

بل إن الرئيس السابق لقسم الأمن الوطني، مايكل تشيرتوف، أثار المخاوف حيال سياسة الخصوصية والنشر لنظارات غوغل، إذ كان يتساءل عن حق عمن يمتلك بيانات فيديو المستخدمين وما إذا كان سيتم تحليل قاعدة بيانات الفيديو هذه برمتها والتنقيب فيها لأغراض تجارية. ومن حق المرء أيضاً أن يسأل عن إمكانية وصول الحكومة إلى هذه البيانات، سواء بشكلٍ رجعي في المستقبل أو في الوقت الحالي، ولأسبابٍ تتنوع من محاربة الجريمة إلى مسائل "الأمن الوطني". لنتأمّل في تبعات الأمر للحظة: باستخدامك لنظارات غوغل، هل تمنح الشركة حق الاستيلاء على كافة اللحظات الحية من حياتك اليومية، أي كل شيء تسمعه وتراه، وتمكنها من بيع هذه البيانات للمعلنين؟ على سبيل المثال، قد يلاحظ نظام نظارات غوغل، أثناء ارتدائك للنظارات وأنت تحضّر قهوة الصباح ببرنس الحمام، جسماً ضمن نطاق رؤيتك كركوة القهوة (وهذا أمر محتمل جداً)، هل من الممكن أن ترى قسائم ستاربوكس من خلال شاشات نظارتك؟ من خلال انتهاكات الخصوصية المذكورة آنفاً، والتي رأينها من عملاق البحث، ما هو

الشيء الآخر الذي بمقدوره فعله طالما أننا ندخل عصر أدوات المراقبة القابلة للارتداء؟

الشبكة الاجتماعية ومخزونها، أنت

لا شك في أن غوغل ليس الوحيد الذي يتبع النموذج التجاري القائم على بيعك للمعلنين، فهناك الآلاف من الشركات حول العالم تقوم بالعمل نفسه، ومن أبرزها فايسبوك. يُعتبر فايسبوك الذي أسسه عام 2004 مارك زوكيربيرغ في غرفة سكنه في جامعة هارفارد، قصة نجاح رمزية بالنسبة لوادي السيليكون. فبوجود أكثر من 1.2 مليار مستخدم فعلي شهرياً، يُعتبر الفايسبوك وإلى حد كبير أضخم شبكة اجتماعية في العالم. ويكمن نجاح الفايسبوك في جعله الناس يتكلمون عن أنفسهم بطرقٍ لم تكن قابلة للتصور من قبل. فمعلومات مثل الميول الجنسية والوضع العائلي والدوام في المدارس وشجرة العائلة وقوائم الأصدقاء، والعمر والجنس وعناوين البريد الإلكتروني ومكان الولادة والأخبار المفضلة والتاريخ المهني، وقوائم الأشياء المفضلة والديانة والانتماءات السياسية والصفقات والصور والفيديوهات، كلها تجعل الفايسبوك حلم المسوقين. يعرف المعلنون أدق التفاصيل عن حياة مستخدم الفايسبوك، ولذلك يمكنهم التسويق له أو لها بدقةٍ متناهية معتمدين في ذلك على البيان الاجتماعي الذي يولّده الفايسبوك.

علاوةً على ذلك، أوجد الفايسبوك عدداً من الابتكارات التي تسمح له بتتبع المستخدمين عبر الشبكة ككل، ومن ضمنها زر الإعجاب الحاضر دائماً. لقد تم تدريبك على الضغط على الزر الأزرق الجذاب، الذي له شكل إبهام مرفوعٍ نحو الأعلى لكي تعبّر عن دعمك لفكرةٍ معينة أو حالة محدّثة أو صورة؛ وفي النهاية، إنه لمن التهذيب فعل شيءٍ كهذا. سيرى أصدقاؤك أنك تدعم رسالتهم، ولكن ما لا ترونه جميعكم هو ما يحدث بالبيانات المتولّدة

عن كل إعجاب، تلك البيانات التي يتم جمعها وتحليلها وبيعها للتجار والسماسرة حول العالم. عندما تستخدم بيانات دخول فايسبوك لزيارة مواقع أخرى على الشبكة، مثل سبوتيفاي وباندورا، يعالج محرك فايسبوك للتنقيب في البيانات أولوياتك، مفضلاً ليدي غاغا على بليك شيلتون، تماماً كما يقوم بتتبع كافة المواقع التي زرتها والتي يوجد فيها رمز الفايسبوك (حتّى لو لم تسجّل دخولك فيها).

إذا كنت لا تشارك قدراً كافياً، فسيكون فايسبوك سعيداً بإيجاد قواعد وقوانين جديدة ليجبرك على المزيد من المشاركة، كما فعل في عام 2012 عندما أسس "ميزة" الخط الزمني الإلزامية. فقد قدم هذا التغيير للمعلنين نافذة فعالة دائمة التحديث، يطلّون من خلالها على الأمور الهامة في حياتك في أي لحظة من الزمن. وأمّن لفايسبوك تغذية بموادّ إضافية يبيعها للمعلنين. لقد سبق لفايسبوك، مثله في ذلك مثل غوغل، أن تعرض للانتقاد على نطاق عريض في مسائل تتعلق بالخصوصية وسلامة الأطفال ولغة الكراهية. ولطالما تعرض للمقاضاة في أنحاء العالم، وكانت آخر هذه المرات في المحكمة الفدرالية الأميركية في سان هوزيه بكاليفورنيا، بسبب "الاعتراض المنظم والمنهجي لرسائل المستخدمين الخاصة... ومشاركة البيانات مع المعلنين والمسوّقين".

ليس غوغل وفايسبوك أبداً الوحيدين اللذين يجعلانك تكشف بياناتك الشخصية ثم يبيعانها: بل ثمة أيضاً تويتر وإنستاغرام وبينتيريست والمئات من الشركات الأخرى. فعلى سبيل المثال، هل كنت تدرك أنه في كل مرة تقوم بها بطرح سؤال على عميل الذكاء الصنعي سيري من شركة أبل، فإن تسجيل صوتك يخضع للتحليل ومن ثم التخزين لدى الشركة ولمدة لا تقل عن سنتين؟ على أية حال، ليس السؤال هو من يخزن بياناتك، فالجميع يمكن أن يفعلوا ذلك هذه الأيام، بل السؤال هو ما الذي يفعلونه بتلك

المعلومات؟ لو كانت الصفقة الفاوستية بسيطة إلى درجة اعتبارها مجرد تبادل بين الخدمات المجانية وبعض البيانات، لكان كل شيء في العالم على ما يرام. لكن الأمور ليست بهذه البساطة. وسرعان ما ستكتشف أن الاحتفاظ بهذه الكميات الهائلة من البيانات وتخزينها في عالم مترابط وتبعي وهشّ على هذا النحو يجعلك عرضة للمخاطر بطرقٍ لم تكن لتتخيلها من قبل.

تسريب المعلومات، كيف يفعلونها

في كل مرة تزور فيها موقعاً إلكترونياً جديداً، يقوم هذا الموقع بوضع ملفات رقمية مخفية مميزة تعرف باسم كوكيز، أو السكاكر، على حاسبك أو هاتفك. من خلال هذه الملفات الصغيرة يصبح من السهل تعقبك وتعقب نشاطاتك عبر الإنترنت. بالإضافة إلى ذلك، لكل من أجهزتك الرقمية بصمتها الخاصة الفريدة، وهذا يجعلك عرضة للتعقب والتصنيف. هنالك عناوين لمحددات فريدة، مثل عنوان بروتوكول الإنترنت (IP) لشبكة الحاسب التي تستخدمها للوصول إلى الإنترنت، ورقم التحكم بالوصول إلى الوسيط (MAC) لبطاقة الشبكة اللاسلكية (Wi-Fi) ورقم IMEI أو رقم I لهاتفك النقال، وجميعها تسمح للشركات الموجودة على الإنترنت بالتعرف بدقة إلى الأجهزة (والمستخدمين) التي تستفيد من خدماتها.

يجري تتبع كافة هذه البيانات وتوحيدها والاستفادة منها، لإعطاء شركات الإنترنت والمعلنين تصوراً واضحاً ومستمراً عنك وعن نشاطاتك على الإنترنت. فوفقاً لدراسةٍ صادرة عن صحيفة وول ستريت جورنال عام 2012، كان أكثر الأعمال التجارية سرعة في النموّ هو التجسس على مستخدمي الإنترنت. وفي التقرير نفسه، ألقي الضوء على خمسين موقعاً من أكثر المواقع شعبية، اكتشف أن كلاً منها يترك وسطياً 64 ملف كوكيز للتتبع لمصلحة المعلنين، لكي يتمكنوا من تتبع ومراقبة فعالياتك على الشبكة.

وأكثر المواقع التي لديها برامج للتتبع هو موقع ديكشيناري، أو القاموس، بإجمالي قدره 234 ملف توضع على حاسبك في كل زيارة تقوم بها لهذا الموقع. جميع هذه المرشدات والملفات التعقبية يتم جمعها من خلال الإعجابات والإشارات والأصوات، لترسم على نحو غريب صورة مفصلة عن شخصيتك الرقمية. ووفقاً للنتيجة، تقوم هذه الملفات الصغيرة الموجودة على حاسبك بتطوير نفسها لتصبح ملفات أضخم تكشف بياناتٍ لم تكن تريد لها في أية حال أن تشاهد من قبل الجميع.

لست أنت الوحيد الذي يسرب بياناتك عبر نشاطاتك الاجتماعية على الشبكة، فأصدقاؤك وعائلتك يقومون بدورهم بتسريب هذه البيانات. ففي كل مرةٍ يقوم فيها صديقٌ لك بوضع اسمك وعنوانك على غوغل كونتاكتس أو آيفون، فإنه يزود شركتي غوغل وأبل بتفاصيل شخصية عنك. سجّل يوم ميلاد ابن أخيك أو أختك أو صديقتك أو زميلك في العمل على موقع آوت لوك كاليندر من مايكروسوفت، وستصبح شركة مايكروسوفت على علم بتاريخ ميلاد الشخص المعني. وعندما يشير أصدقاؤك إليك في صور حفلةٍ على الفايسبوك (بعد أن تكون قد أخذت إجازة مرضية من العمل) يكونون قد شاركوا موقعك مع المسوّقين وربما مع بقية العالم، بما فيهم رئيسك في العمل. تسعد الوسائط الاجتماعية وشركات الإنترنت بأن يقوم المستخدمون بهذا العمل لأجلها؛ فالأمر أشبه بامتلاك قدرة مجانية تدأب على تعبئة استمارة تلو الأخرى لتغذي بها آلات البيانات الكبيرة.

بل إن الأمر نفسه يحدث عندما يستخدم صديق لك موقعاً إلكترونياً أو خدمة لا تستخدمها أنت. فعلى سبيل المثال، بالنسبة لأولئك الذين ليس لديهم حساب على جيميل بينما يمتلك أصدقاء لهم مثل هذا الحساب، فإن إرسال رسالة إلى أي مستخدم من مستخدمي جيميل البالغ عددهم 425 مليوناً يعني أن غوغل الآن أصبح طرفاً في حديثك. لذا فإنك إذا استخدمت

عنوان بريدك الإلكتروني الخاص بالعمل أو الجامعة لترسل رسالة إلى أختك على حسابها على جيميل، وحتى لو لم تفتح حساباً لك على غوغل، فإنه يستمر في قراءة وفحص الرسالة وفي البحث عن كلماتٍ تهمه يمكن بيعها إلى المعلنين، وهي الممارسة التي تعرّض الموقع للمقاضاة حالياً في المحكمة الفدرالية. في مذكرة الدفاع عن نفسه في الدعوى القضائية التي رفعتها القاضية لوسي كوه، كانت الصدمة في أن يعلن غوغل أن "ليس للشخص أن يتوقع خصوصية قانونية في المعلومات التي يقدمها طواعية لأطراف أخرى". بعبارة أخرى، الحجة التي يقدمها غوغل هي أنه في حال إرسال أية رسالة إلى أحد مستخدمي جيميل، فإنني أقوم تلقائياً بالتنازل عن حقوق الخصوصية وأقبل بما يقوم به غوغل من استيلاءٍ وبيعٍ للرسالة ومضمونها، حتى ولو كان قصدي أن تكون الرسالة خصوصية وحتى لو لم يكن لدي حساب على جيميل.

ليس أصدقاؤك الوحيدين الذين بسربون بياناتك لفريق ثالث مثل غوغل، فأطفالك يقومون بذلك أيضاً. في الحقيقة، فإن المواقع تستهدف الأطفال لأنهم ينصّبون تكنولوجيات التعقب على حواسبهم أكثر من الكبار. وبالرغم من أن القانون الفدرالي الذي يحمل اسم قانون حماية خصوصية الأطفال على الإنترنت، حدّ من المعلومات التي يمكن أن يجمعها المسوقون للأطفال الذين هم تحت سن الثالثة عشرة، فإن القانون يتعرض بشكل روتيني لانتهاكات صارخة. إذ يتلقى الأطفال وبشكلٍ مستمر طلباتٍ للمشاركة في منافسات وألعاب وللإجابة عن استطلاعات رأي، في محاولةٍ لانتزاع المزيد والمزيد من بياناتهم، في انتهاكٍ واضح للقانون الفدرالي. وقد تعرضت شركات مشهورة مثل ماكدونالدز وجنرال ميلز وفياكوم وتورنر برودكاستينغ سيستم وصابوي للغرامة، بسبب انتزاعها البيانات من الأطفال من خلال مواقعها ذات التصميم الكرتوني مثل HappyMeal.com

وReesesPuffs.com وNick.com وsubwayKids.com. وفي قضية أخرى، طلبت شركة سوني بي.إم.جي ميوزيك من القاصرين إدخال عناوين الشوارع التي يسكنونها وأرقام هواتفهم في صفحات الإعجاب الخاصة بفرقهم المفضلة، ثم قامت شركة سوني ببيع هذه المعلومات لسماسرة البيانات في ثلاثين ألف حالة على الأقل، ودون الحصول على موافقة الأهل كما هو منصوص عليه في القانون الفدرالي. ولكن لماذا تقوم شركاتٍ موقرة مثل ماكدونالدز وغوغل وفايسبوك وجنرال ميلز وسوني بمثل هذه الأفعال؟ من السهل تحديد السبب، فهناك مبالغ هائلة من الأموال في هذه اللعبة، وبالنسبة لهم، أي الشركات، تستحق أنت وبياناتك المجازفة نظراً لما يمكن تحقيقه من عوائد هائلة.

أغلى الأشياء في الحياة هي أشياء مجانية

الفرضية التجارية التي لا يفهمها معظم مستخدمي الإنترنت، هي أنهم يدفعون بالفعل مقابل ما يُسمى الخدمات المجانية التي يتلقونها على الإنترنت، بل يدفعون ثمناً باهظاً. فذلك الصوت الخافت الذي تسمعه هو صوت خصوصيتك وصوت بياناتك وكافة التفاصيل التي تشكل هويتك المميزة، وهي تُبتلع من قبل نظام الشفط الضخم المرافق للإنترنت. فتفاصيل عمليات البحث التي تقوم بها، والتي لا تحلم بمشاركتها مع أقرب أصدقائك وأفراد عائلتك، تتم تصفيتها من قبل خوارزمية حاسوبية كبيرة في الفضاء، وجمعها في مجموعات يقدر حجمها بالبيتابايت لتُباع بالمليارات. ولهذا تحصل على بحثٍ مجاني فيما تصل قيمة غوغل إلى 400 مليار دولار. فالفضل في كل ذلك يعود لك أنت، سلعته. تلك هي الصفقة التي قمت بها سواء كنت تدرك ذلك أم لا.

بلغ إجمالي عوائد غوغل في عام 2013 أكثر من 59 مليار دولار. وهي قيمة تمثل الفرق بين قيمة خصوصيتك بالنسبة لمعلني غوغل وبين القيمة

التي لم تُدفع لك. أي إن غوغل يحصل على 59 مليار دولار، بينما تحصل أنت على بحثٍ وبريد إلكتروني مجانيّين. فقد نشرت صحيفة وول ستريت جورنال دراسة سبقت عرض أسهم فايسبوك في السوق، قدرت فيها قيمة كل مستخدم دائم للفايسبوك بـ 80.95 دولاراً للشركة. تبلغ قيمة صداقاتك اثنين وستين سنتاً لكل واحدة، وصفحة حسابك 1.800 دولار. كما بلغت قيمة صفحة إلكترونية تجارية وما يرتبط بها من دخل إعلاني تقريباً 3.1 مليون دولار، تعود للشبكة الاجتماعية.

وبالنظر إلى الموضوع من زاوية أخرى، يقوم المليارات من مستخدمي الفايسبوك طوعاً، بتحديث حالاتهم على الموقع وبتقديم التفاصيل عن سيرهم الذاتية وبوضع الصورة تلو الأخرى، وهذا جعلهم أكبر قوة عاملة غير مأجورة على مر التاريخ. فنتيجة لعملهم المجاني، يتمتع الفايسبوك بقيمةٍ سوقية تصل إلى 182 مليار دولار، وصار لدى مؤسس الموقع، مارك زوكيربيرغ، شبكة خاصة تبلغ قيمتها 33 مليار دولار. فما الذي حصلت عليه من هذه الصفقة؟ كما يذكرنا عالم الحواسب جارون لانير، فإن شركة مثل إنستاغرام، التي اشتراها الفايسبوك عام 2012، لا تبلغ قيمتها مليار دولار لأن موظفيها الثلاثة عشر كانوا استثنائيين. بل تستمد هذه الشركة قيمتها من ملايين المستخدمين، الذين يسهمون في الشبكة بدون مقابل مالي. فلا يحتوي مستودع هذه الشركة سوى على البيانات الشخصية، العائدة لك أو لي، وتقوم الشركة ببيعها مراراً وتكراراً لأطراف مجهولة حول العالم. باختصار، أنت شخص ضعيف لا قيمة له كان يقوم، وبرضاه التام، بتزويد شركات الإنترنت بكل شيء يعرفه ويقوم به وبكل مكانٍ يذهب إليه مقابل بعض الراحة والتسلية.

كأن صفقة المال مقابل البيانات لم تكن قاسية بما فيه الكفاية بالنسبة لغوغل، لذلك قررت الشركة زيادة القيمة المقدرة بـ 400 مليار دولار عن

طريق استخدامك أنت وصورك في إعلاناتها. ففي تشرين الأول من عام 2013، أعلنت الشركة ميزة جديدة تُسمّى التزكيات المشتركة، بدأت تظهر في نتائج البحث والخرائط وغوغل بلاي ستور. فمثلاً، إذا قمت بمنح أغنية على غوغل بلاي خمس نجوم أو أبديت إعجاباً داعماً لحانة أو مخبز محلي، فإن غوغل الآن يكون قد منح نفسه حق بيع الإعجاب والاسم والإقرار لشركات الإعلان وسماسرة البيانات. بالطريقة نفسها، عندما يقوم صديقاك تشارلي وجوانيتا بالبحث عن حانة أو أغنية في غوغل، فإنهما سيريان وجهك المشع يزكّي المنتج إلى جانب من نتائج بحثهما. كان جورج كلوني وأنجيلينا جولي يتلقيان المال مقابل تزكياتهما المنتجات بين معجبيهما، لكن ماذا عنك؟

قدم غوغل "التزكيات المشتركة" بعد برنامج مشابهٍ إشكالي جداً اسمه "القصص الممولة"، أسسه فايسبوك وعن طريقه استخدمت الشركة إعجاباتك لتزكّي زبائنها الحقيقيين، أي المعلنين والمنتجات التي يمثلونها. وبعد أن تم رفع دعوى قضائية جماعية ضد فايسبوك، ألغت الشركة الميزة المثيرة للجدل، ولكن ليس قبل أن تجني 230 مليون دولار في الأشهر الثمانية عشرة، التي شغّلت فيها هذا البرنامج. وفي النهاية، سوّى فايسبوك الدعوى بدفعه 20 مليون دولار، أو ما يعادل سِنْتين لكل مستخدم. ربما كنت تتساءل الآن كيف أمكن لهم أن يفلتوا من العقاب على هذا العمل؟ الجواب بسيط: لقد تمكنوا من ذلك وقضي الأمر كما قلت توًّا.

الأحكام والشروط مطبقة (ضدك)

"قرأت شروط الخدمة ووافقت عليها"، هي أكبر كذبة على الإنترنت.

شروط الخدمة: لم تقرأ HTTP://TOSDR.ORG

جميعنا رأى تلك الشروط. تلك التنازلات مستحيلة الطول، المكونة من خمسين صفحة مكتوبة بخط صغير جداً دون ترك فراغات بين الأسطر وبهوامش يبلغ قياسها **1/8** إنش. لقد صُممت بهذا الشكل لتستحيل

قراءتها، لذا فإننا لا نقرأها. لا نقرأها ولا نفهمها، الأمر الذي يكلفنا ثمناً باهظاً. توجد شروط الخدمة هذه في الوقت الحالي في كل موقعٍ إلكتروني وفي كل عقدٍ من عقود الهواتف الخلوية، وفي كل اشتراكٍ في تلفاز الكابل أو طلب بطاقة ائتمانية. وتوضح هذه الشروط كيفية إمكانية انتزاع البيانات الشخصية منك واستخدامها بطرق لا يمكنك تخيلها، ومن بينها طرق ربما كنا سنعترض عليها لو أننا تمكنا بالفعل من فهم الاتفاقية التي نوافق عليها.

وفقاً لدراسة صادرة عن جامعة كارنيج ميلون، يواجه كل أميركي في كل سنة ما يقارب 1.462 وثيقة متعلقة بالخصوصية، وكل وثيقة تتكون مما يقارب 2518 كلمة. فلو أراد كل شخص أن يقرأ كل واحدة من هذه الوثائق، لاستغرقه ذلك ستة وسبعين يوماً، بمعدل ثماني ساعات كل يوم. ويصل المجموع إلى 53.8 مليار ساعة لكافة الأميركيين، بتكلفة تقدر بـ 781 مليار دولار على المستوى القومي تمثل خسارة في الإنتاجية السنوية ناتجة عن كابوس وفضيحة اسمها شروط الخدمة.

لو كانت المسألة تتعلق بالإنتاجية الضائعة فقط، لما كانت فضيحة كبيرة بالطبع، لكن هذه السياسات ستؤثر على محفظتك بشكلٍ مباشر أيضاً. فقد قدرت دراسة صادرة عن صحيفة وول ستريت جورنال أن اللغة المتحيزة تماماً في وثائق شروط الخدمة تكلف كل مواطن أميركي عادي 2000 دولار في السنة، بإجمالي قدره 250 مليار دولار سنوياً، وهي أموال تم خداعنا بها بعد أن تم ترتيب جميع الأوراق بحيث يمكن استخدامها ضدنا. وبالرغم من أن الشركات تطلق على هذه الأحكام اسم شروط الخدمة، فإنها من وجهة نظر المستهلكين تستحق عن جدارة اسم "شروط الاستغلال".

لنأخذ مثالاً عن التكلفة الناجمة عن استخدامك موقعاً للوسائط الاجتماعية، مثل موقع لينكدإن الذي تنص سياسته المتعلقة بالخصوصية على ما يلي:

> إنك تمنح موقع لينكدإن الحق العام والنهائي والواسع والدائم والمطلق والمخصص، والقابل لإعادة الترخيص والمأجور والمتحرر من قيود النشر، يخولنا بأن ننسخ ونحضر ونشتق ونحسّن ونوزع وننشر ونزيل ونحفظ ونضيف ونعالج ونحلل ونستخدم ونتاجر بأي طريقة معروفة الآن أو ستُعرف في المستقبل، أية معلومات تقدمها بشكلٍ مباشر أو غير مباشر لموقع لينكدإن تشتمل، ولكن لا تنحصر بـ: أية محتويات و/أو أفكار أو مفاهيم أو تقنيات أو بيانات للخدمات ينشئها أي مستخدم ويحملها على موقع لينكدإن، دون أية موافقة إضافية أو ملاحظة أو تعويضات لك أو لأي طرفٍ ثالث. أية معلومات تقدمها لنا أنت تتحمل خطر فقدانها.

أي إنك باستخدامك لموقع لينكدإن، تمنحه نفوذاً مطلقاً ودائماً (ومجانياً) للوصول إلى أية معلومات وضعتها على الموقع؛ ولا يمكنك التراجع أو البدء من جديد. وحالما يحصل الموقع على بياناتك وعلى بيان شبكتك الاجتماعية وعلى تاريخ عملك ومهاراتك ومستوى تعليمك، يمكنه بيعها في الحال أو في المستقبل بأية طريقة يفضلها، بما في ذلك طرق لم تُعرف بعد (كأن يمتلك حقوق الهولوغراف على صورك بما يمكنه من استخدامها في الإعلان؟). لإيضاح كم أصبحت سياسات الخصوصية تافهة في النهاية، قامت شركة التجزئة البريطانية غيم ستيشن بإطلاق تجربة لترى إن كان أحدٌ يقرأ شروط الخدمة. حيث قامت الشركة المذكورة بتعديل سياسة الخصوصية بحيث أصبحت سهلة القراءة:

> بوضعك أمراً من خلال موقع غيم ستيشن في اليوم الأول من الشهر الرابع لعام 2010 ميلادي، فإنك توافق على

منحنا خياراً غير قابل للتحويل حالياً وإلى الأبد يمكننا بموجبه طلب روحك الخالدة. عندما نرغب بتطبيق هذا الخيار، فإنك ستوافق على تقديم روحك الخالدة، وأي طلب تتلقاه في هذا الخصوص، ضمن خمسة أيام من تلقيك إشعاراً مكتوباً من موقع gamestation.co.uk أو أحد محبيه المُفوّضِين حسب الأصول.

صحيح، لقد قام خمسة وسبعون بالمئة من زبائن غيم ستيشن ممن قاموا بشراء شيء عن طريق موقع الشركة في اليوم الأول من انطلاق التجربة، بتقديم أرواحهم الخالدة بشكلٍ نهائي إلى هذا البائع البريطاني. لكن فيما تؤكد التجربة الفرضية المقترحة، فإن شروط الخدمة ليست أمراً مضحكاً، فالمحاكم في مختلف أنحاء العالم تجد أن نقرك بالفأرة على الاتفاقية تعتبر مُلزمة من الناحية القانونية، مع كل ما تحمله من تبعات مالية وخصوصية وأمنية بالنسبة لك.

لدى جميع شركات الإنترنت تقريباً السياسات الوحشية نفسها التي تعمل ضدك. وفيما أن معظم هذه الشركات تكاد تطالب بالفعل بروحك الخالدة، فإن العديد منها يقترب من ذلك إلى حد ما، وكلما استُخدمت كلماتٌ أكثر، ازداد الأمر سوءاً بالنسبة لك. فعلى سبيل المثال، ازداد عدد كلمات سياسة الخصوصية على فايسبوك من 1004 كلمات عام 2005 إلى 9300 كلمة عام 201 (وذلك دون حساب عدد الروابط لمختلف السياسات الفرعية والشروط الأخرى). ولوضع ذلك في منظوره الصحيح، فإن سياسة الخصوصية للفايسبوك أطول بمرتين أو أكثر من الدستور الأميركي. في الوقت عينه، تعتبر سياسة الخصوصية لشركة بي بال والتعديلات التي طرأت عليها أطول وثيقة في هذه الصناعة، إذ تتألف من 36,275 كلمة. وإذا أردنا المقارنة، فإن مسرحية هامليت لشكسبير تتألف من 30,066 كلمة من بينها عبارة

مناجاة النفس "نكون أو لا نكون"، والخطاب المؤثر "عمت مساءً أيها الأمير اللطيف" في النهاية. بل ثمة مسائل أكثر تعقيداً، فالفايسبوك وغيره من الشركات تمنح نفسها حقوق تغيير وثائق الخصوصية عندما ترغب وهم يقومون بذلك دائماً.

والأسوأ من ذلك هو أن معظم الشركات تضع إعداداتٍ يستحيل الوصول إليها وفهمها لوثائق الخصوصية، فلدى الفايسبوك مثلاً خمسون نقطة تتعلق بإعدادات الخصوصية تتشعب أيضاً إلى 170 خياراً، وهي بعيدة كل البعد عن الفهم بالنسبة لإنسانٍ عادي، وهنا تحديداً تكمن الغاية منها. علاوةً على ذلك، وحتى لو أضعت الساعاتٍ التي يتطلبها تنظيم إعدادات الخصوصية لحسابك، فإن أية تحديثات يقوم بها الفايسبوك لشروط الخدمة تؤدي وبشكلٍ تلقائي إلى إعادة كافة المستخدمين إلى الإعدادات التلقائية، والتي تُعتبر أعلى مستوى في الانفتاح (لذلك يمكنه بيع المزيد من سلعه، أي مستخدميه، لزبائنه الحقيقيين، أي المعلنين). إذا لم تقم بتفقد الإعدادات الخاصة بك، كما يفترض بك، فستجد أن الفايسبوك تجاهل بالجملة رغباتك المتعلقة بالخصوصية التي كنت قد وضعتها صراحةً. نتيجة لذلك، يحتفظ الفايسبوك لنفسه بسلطة استغلالك تجارياً دون تضارب أو تنافر من خط تجميع السلع البشرية الصاخب الذي يديره.

بعد ثلاثة أشهر من شرائه من قبل فايسبوك، أغضب إنستاغرام مستخدميه عندما أعلن أنه سيبيع أسماءهم وصورهم للمعلنين. فوفقاً لشروط الخدمة المحدثة، يقول إنستاغرام إن الآباء الذين يضعون صوراً لأطفالهم الصغار على موقعه يقبلون ضمنياً باستخدام هذه الصور في الإعلانات. وبذلك بات من الممكن لصورة ابنك الرضيع التي وضعتها لتشاركها مع والديك أن تُستخدم الآن لبيع أطعمة الأطفال، لأن إنستاغرام منح نفسه تلك الحقوق. والصورة الرائعة التي التقطها لغروب الشمس

فوق مانهاتن يمكن أن تُباع كصور مجردة للصحف والمجلات. نتيجة تغييره لشروط الخدمة، أصبح ستة عشر مليار صورة عائدة للمستخدمين ملكية فكرية لإنستاغرام، الأمر الذي يوضح ما دفع فايسبوك لدفع مليار دولار لشركة مؤلفة من ثلاثة عشر موظفاً فقط.

حتى غوغل لم يتورع عن تطبيق شروطٍ خدمة تافهة كهذه. فأي شخص يستخدم مستندات غوغل أو حدث أن قام بتحميل جداول بيانات وملفات بي.دي.إف أو ملفات وورد على غوغل درايف على سبيل المثال، يمنح تلقائياً ملكية هذه الوثائق لغوغل. فوفقاً لشروط الخدمة لدى غوغل:

> "عندما تقوم بتحميل أو وضع مادة معينة على خدماتنا، فأنت تعطي غوغل (وأولئك الذين نعمل معهم) رخصة عالمية لاستخدام واستقبال واستنساخ وتعديل أو إنشاء أعمال مشتقّة، كتلك الناتجة عن الترجمات والتعديلات أو غيرها من التغييرات، كما تمنحه رخصة المشاركة والنشر والتنفيذ والعرض والتوزيع العلني لمثل هذه المواد".

فكّر في ذلك، لو أن ج.ك.رولينغ كتبت هاري بوتر باستخدام غوغل دوكس بدلاً من مايكروسوفت وورد، لكانت منحت غوغل صلاحيات واسعة على عملها، أي الحق في تعديل وتكييف شخصيات الموغل كما يرتئي غوغل، ناهيك بمدرسة هوغوارتس للسحر والعرافة. كما أن غوغل كان سيحتفظ بحقوق بيع قصصها إلى استوديوهات هوليوود ليتم تمثيلها على المسارح حول العالم، بالإضافة إلى امتلاكه كافة حقوق الترجمة. لو أن رولينغ كتبت روايتها الملحمية في غوغل دوكس، لكانت قد منحت غوغل الحق في 15 مليار دولار هي عوائدها من إمبراطورية هاري بوتر، وكل ذلك استناداً لما تنص عليه شروط الخدمة.

قد يشكل قيام فايسبوك وغوغل وتويتر وغيرها بتخزين بياناتك الموجودة

على الشبكة واستثمارها إلى أبعد حد ممكن، مفاجأة صغيرة الآن. لكن المفاجأة على كل حال تكمن في العدد المتزايد للمنصات التي يمكن من خلالها للمعلنين جمع ومعالجة هذه المعلومات، كالهاتف الذي كان ذات يوم جهازاً متواضعاً. كان ألكسندر غراهام بيل سيُصاب بالصدمة لو أنه شاهد اختراعه وهو يتحول اليوم إلى جميع هذه الهواتف الذكية وتطبيقاتها التي تتغلغل في حياتنا مشكلة مخاطر لا يستهان بها على خصوصيتنا وحرياتنا.

أنا، المحمول

> نعم، هاتفي. عندما ظهرت هذه الأجهزة لأول مرة كانت لطيفة. لكن أحداً لم يدرك، إلا بعد فوات الأوان، أنها لا تختلف في شيء عن شرائح تعقب إلكترونية تزرع في السجناء في الحبس الاحتياطي.
>
> دافيد ميتشيل، رواية "كتبته الأشباح"

يوجد على هذا الكوكب حالياً من أجهزة الهاتف الذكية أكثر مما يوجد من البشر، والنتيجة هي هذا الغطاء الرقمي الدائم الحضور الذي بدأ بتغليف الأرض على نحو يطال الجميع بتبعاته. وما هذه الهواتف الذكية اليوم سوى حواسب مصغرة قوية نحملها معنا على مدار الساعة لتشكل جزءاً لا غنى عنه من حياتنا. وقد اعترف ثلاثة وستون بالمئة من الأميركيين بأنهم يتفقدون هواتفهم في كل ساعة، بينما يتفقد حوالى 10 بالمئة أجهزتهم كل خمس دقائق. ترافقنا هذه الأجهزة إلى الحمام وقاعات الرياضة وغرف النوم، وقد احتلت مكان الكاميرات والحواسب والآلات الحاسبة ومفكرات التقويم ودفاتر العناوين وأجهزة الراديو والتلفزيون والألعاب. بل إن إجراء الاتصالات لا يمثل في الحقيقة أكثر من خُمس النشاطات العامة التي يستخدم الناس من أجلها أجهزتهم الذكية، بعد تصفّح الإنترنت وشبكات التواصل الاجتماعي وممارسة الألعاب والاستماع

إلى الموسيقى. وتمثل هذه الآلات الصغيرة جزءاً متكاملاً من حياتنا، إذ يعترف 84 بالمئة منّا أنهم لا يستغنون ولو ليوم واحد عن الهاتف. وتُعتبر الهواتف الذكية صديقنا الصدوق، وهي لذلك تتمتع بخاصية الوصول اللامحدود إلى حياتنا اليومية. ولكن هل تم السماح بهذا المنفذ إلى حياتنا دون اعتبارٍ كافٍ لما يعنيه ارتباطنا بحاسب نحمله معنا بالفعل على مدار الساعة؟

صحيح أن هذه الأجهزة مفيدة ودائمة الحضور في حياتنا، إلا أنها أيضاً أجهزة تنصت حقيقية نحملها في جيوبنا، إنها جواسيس رقمية تتتبع تحركاتنا في كل مكان. ذلك الجهاز الموجود في حقيبتك أو في بنطالك، والذي تظنه هاتفاً خلوياً، ما هو في حقيقة الأمر سوى مرشد لاسلكي يومئ للعالم باستمرار ويقدم فيضاً مستمراً من البيانات المتعلقة بك وبموقعك وبنشاطات حياتك. ففي الولايات المتحدة وحدها، تقوم أجهزة الهاتف المذكورة بإنتاج حوالى 600 مليار حدث مزوّد بمعرف مميز كل يوم، تشمل بيانات عن مكانك وعن الشخص الذي تراسله وكذلك الصور التي قمت بتحميلها. يبدو حجم البيانات التي نسربها بواسطة حواسبنا في المنزل أو في العمل تافهاً إذا ما قورن بحجم البيانات التي نسربها عبر أصدقائنا الرقميين الذين نحملهم في جيوبنا. إذ تُقدم الهواتف النقالة الصورة الأوضح لعادات أو أولويات أي شخص مخترقةً حياته بكل معنى الكلمة. فمن يصل إذاً إلى كل هذه البيانات؟ هؤلاء أكثر بكثير مما تعتقد. فمعرفة مكانك وأين أمضيت وقتك وصرفت نقودك ومع من يمنح فرصاً أكبر للتنقيب في حياتك تنقيباً أعمق ولتحويل هذه المعلومات إلى مال. كما أن سماسرة البيانات والجواسيس والمجرمين ينظرون بدورهم إلى الهواتف الخلوية على أنها مصدرٌ غني لتبادل المعلومات المفيدة عن أهدافهم. لذلك فإنهم، مثلهم مثل غيرهم، يتتبعون الهاتف الذكي بكل ما أوتوا من عزم.

كانت فرصة الحصول على كافة بيانات جهازك الخلوي هي التي دفعت غوغل إلى تطوير نظام تشغيل أندرويد للهاتف النقال، وتقديمه مجاناً للمطورين والمستخدمين. ولكن كما رأينا سابقاً، يمكن للشيء المجاني أن يكون عرضاً مكلفاً جداً. إذ يقوم أندرويد الموجود في الهواتف النقالة بتزويد غوغل برقم هاتفك وبمعلومات عن شبكتك وبالبيانات المخزنة على الجهاز وبسجلات المكالمات وبقوائم الاتصالات، إضافة إلى إمكانية الوصول إلى مجموعة من الحساسات الجديدة بإمكانها اكتشاف حركتك وموقعك، وحتى الشروط المحيطة بك كالحرارة والرطوبة ومستويات الأصوات. بعد أن أدخل غوغل كل هذه الأشراك التقانية إلى حياتك، لم يضع أي لحظة وسارع إلى التقدم بطلب براءة اختراع عما سماه "الإعلان المعتمد على العوامل البيئية". رائع! يستطيع غوغل الآن أن يكتشف ما إذا كنت في مكانٍ حار، ليقدم لك وفقاً لذلك إعلاناً عن تكييف الجو أو البوظة. وباستخدام تقنية الصوت المحيط، يستطيع غوغل أيضاً التنصت على مكالماتك الهاتفية للتعرف على الأصوات التي في الخلفية ليقدم إعلاناته وفقاً لتلك التفضيلات. فمثلاً، إذا كنت تستمع لآشر أثناء الحديث مع العمة مارغريت على هاتف أندرويد، فإن غوغل لديه القدرة على اكتشاف ذلك ليعرض لك إعلاناً عن حفلات هذا المغني المقبلة عندما تتفقد بريدك على جيميل في المرة القادمة أو تقوم بالبحث على الإنترنت.

قام الفايسبوك أيضاً بإضافة هذه المقدرة على استخدام ميكروفون هاتفك للتنصت عليك وعلى الأصوات المحيطة بك، وكل ذلك مصرح به في شروط الخدمة المُحدّثة، ويشكل جزءاً من حملته الكبيرة التي تستهدف مستخدمي الهاتف النقال. وعندما كشف الفايسبوك في الربع الأخير من عام 2013 عن وصوله إلى 945 مليون مستخدم للهاتف النقال شهرياً، وأن 53 بالمئة من دخله الآن يأتي من إعلانات الهواتف النقالة، أغدقت البورصة

بحبها على الشركة، مضيفة مليارات الدولارات لقيمته التقديرية خلال الأيام التي تبعت الإعلان. فباختراعه أخيراً للتطبيق الخاص به على الهواتف النقالة، لا يكون فايسبوك قد ابتكر التجربة الأفضل للمستخدمين وحسب، بل أداةً جديدة للحصول على كمياتٍ ضخمة من البيانات من أجهزة المستخدمين الخلوية.

اختلاس بياناتك؟ ثمة تطبيق لذلك

من المعروف أن إعلاناً تجارياً لآيفون عام 2009 قد روّج عبارة "ثمة تطبيق لذلك"، كوسيلة لإيضاح أنه يوجد تطبيق آيفون لكافة احتياجات البشر المحتملة. وكان ذلك تصريحاً جريئاً في وقته، لكن لعل ستيف جوبز كان محقاً فيه. فمنذ إطلاقه عام 2008، تم تحميل أكثر من خمسة وستين مليار مادة من متجر تطبيقات أبل، عادت بأرباح تتجاوز 10 مليارات دولار في سنة 2013 وحدها. ولمنافسةِ أبل، أطلق غوغل متجره الخاص والمعروف باسم غوغل بلاي، وتؤوي كل شركة أكثر من مليون تطبيق مستقل متاحة للتحميل. وكان معدل النمو لهذه البرامج الصغيرة المعروفة باسم التطبيقات استثنائياً، لكن ما هو الشيء الذي يدفع عشرات الآلاف من المطورين حول العالم لإنشاء هذه التطبيقات؟ المال طبعاً، ولكن كيف يجنون الأموال مع أن أغلبية التطبيقات مجانية؟ حسنٌ، كما رأينا من قبل، المنتج المجاني هو نموذج تجاري عظيم، طالما أنك تجني المال من الناس عن طريق الاستيلاء على بياناتهم الشخصية بالجملة. وقد اتضح أن التطبيقات هي بيئة ممتازة لتحقيق ذلك، الأمر الذي يفسر ربما تحول شركات عديدة مثل شركة روفيو (منتجة اللعبة الأشهر "الطيور الغاضبة") من شركة مغمورة إلى شركة تقدر قيمتها المالية بـ 9 مليارات دولار في غضون سنوات قليلة فقط.

وبالطريقة نفسها التي يُنظر فيها إلى السجائر على أنها مجرد أنظمة

فعالة لنقل النيكوتين للجسم، كذلك التطبيقات هي مجرد أدوات منظمة فعالة عالية الكفاءة لنقل بياناتك الشخصية إلى المعلنين (بالرغم من أن السجائر على الأقل مقوننة). إن كمية المعلومات التي تُختلس من هاتفك النقال عن طريق التطبيقات مذهلة. فبمجرد تنصيبك لتطبيق الفايسبوك على هاتف أندرويد يقوم التطبيق آلياً بمشاركة رقم هاتفك مع الشبكة الاجتماعية، حتى قبل أن يدخل المستخدم إلى الخدمة لأول مرة أو حتى قبل أن يوافق على شروط الخدمة. وحالما يتم تحميل الفايسبوك، يوافق المستخدمون عبر شروط الخدمة على منح التطبيق سماحية "التقاط الصور والفيديوهات باستخدام الكاميرا"، مما يسمح للفايسبوك بتشغيل كاميرا هاتفك في أي وقت دون تأكيدٍ منك. وتسمح له شروط الخدمة أيضاً بقراءة نصوص رسائلك. بل إن فايسبوك بدأ مؤخراً يطلب من مئات الملايين من مستخدمي تطبيقه النقال أن يسمحوا لميزته الجديدة "مزامنة الصور" بتحميل كل صورة ملتقطة بالهاتف تلقائياً على مخدمات بيانات الشبكة الاجتماعية الواسعة.

وعلى الرغم من أن الفايسبوك يكفل ألا يشغل هذا التطبيق الكاميرا وألا يقرأ الرسائل، فأنه يحفظ لنفسه الحق بالقيام بذلك. لكن بصراحة، كيف يمكن لأي مستخدم أن يعرف حقيقةً ما هي البيانات التي أُخذت من هاتفه؟ فكل ذلك يتم في الكواليس مخفياً في ثنايا التطبيق ولا يراد له أن يكون مرئياً من قبل أولئك الذين يحولهم فايسبوك إلى منتج خاص به.

يتم الاستيلاء على المعرف الشخصي المميز لك في اللحظة التي توافق فيها على تحميل التطبيق. فمثلاً، عندما تقوم بشراء تطبيق أندرويد من متجر غوغل للتطبيقات، يزود غوغل الشركة صاحبة التطبيق باسمك الكامل وعنوان بريدك الإلكتروني ومكان إقامتك. يحدث هذا دون تنبيه صريح في كل مرة تحمل فيها تطبيقاً معيناً. ولكن من هي بالضبط هذه الشركات

صاحبة التطبيقات، والتي يوجد الآلاف منها حول العالم، مَن أصبح يمتلك الآن اسمك وعنوانك ورقم هاتفك؟ ما هي سياسات الخصوصية لديها، وماذا تفعل بهذه المعلومات؟ ما هي درجة الأمان المتوفرة عند تخزين هذه المعلومات، وإلى من يتم بيعها؟ الحقيقة هي أن "الغرب المتوحش" هو السائد هنا، وقليلة هي، إن وجدت، الضوابط التي يمكنها بشكلٍ فعال حمايتك وحماية بياناتك من هذا الفريق الثالث، أي بائعي المعلومات. وبمشاركة ملايين التفاصيل المتعلقة بملايين الأسماء والاتصالات مع بائعي التطبيقات، يزيد غوغل من احتمال تسريب أو سرقة أو سوء استخدام بياناتك.

لا بد أن الشك قد بدأ يساورك، فألعاب شركة زينغا الواسعة الانتشار على الفايسبوك مثل FarmVille وTexas Hold 'Em Poker وMafia Wars هي مجانية أيضاً لأنها توضع للتنصت على معلوماتك الشخصية، بما فيها أسماء جميع أصدقائك على الفايسبوك. إذ تباع هذه المعلومات إلى العديد من شركات الإعلان والتتبع على الإنترنت، حتى لو كانت إعدادات الخصوصية وضعت على أعلى درجات الحماية. فقد يبدو مسلياً أن تضع الطيور على المقلاع وتقذفها على الخنازير سارقة البيض، كما أكد مليارات الناس ممن حملوا تطبيق لعبة "الطيور الغاضبة"، لكن لهذه اللعبة مقدرة عالية على جمع المعلومات الخاصة بمستخدميها، بما فيها كافة الأماكن التي يذهبون إليها بصحبة هواتفهم النقالة. بل إن دراسة أجريت من قبل مؤسسة كارنيج ميلون للتفاعل بين البشر والحاسب، بيّنت أن خمسة بالمئة فقط من مستخدمي لعبة الطيور الغاضبة كانوا يعلمون أن الشركة كانت تخزن البيانات المتعلقة بأماكنهم لكي تلاحقهم على أرض الواقع لأغراض إعلانية موجّهة. لكن لعبة الطيور الغاضبة ليست وحدها المذنبة، فقد أشار تقرير لشركة مكافي إلى أن 82 بالمئة من تطبيقات أندرويد تتتبع نشاطاتك

المباشرة على الشبكة، وأن 80 بالمئة، وهي نسبة صاعقة، تجمع معلومات الموقع لمستخدميها.

الموقع، الموقع، الموقع

ثمة ثلاثة أسئلة أساسية بالنسبة للمعلنين: من سيشتري سلعهم، وما الذي يبحث عنه الزبائن، وأين هم هؤلاء الزبائن؟ أما في عالم الإنترنت، فقد ربح غوغل سؤال الـ "ماذا" منذ وقتٍ طويل بفضل محركات البحث القوية. إذ يعلم غوغل ما الذي تبحث عنه، بل إنه يملأ صندوق البحث الموجود في أعلى الشاشة قبل أن تُنهي كتابة سؤالك. بينما استأثر فايسبوك بسؤال الـ "من"، فهو يعرفك ويعرف شبكتك الاجتماعية بعمقٍ أكثر من أي شركة أخرى. لكن كلمة "أين" ما زالت طليقة بعيدة عن متناول أي شركة، والمعركة مستعرة بين الجبابرة الموجودين وبين صنف جديد من الشركات الناشئة التواقة للاستئثار نهائياً بسؤال الـ "أين". فتخصيص إعلان أو قسيمة لشراء لبن مثلج لك عندما تقترب من بينكبيري هو الحلم النهائي للمعلنين. وإذا كانت التقنية اللازمة للقيام بمثل هذا الأمر غائبة حتى الآن، فإن الأمر قد تغيّر مع ثورة الهواتف النقالة، ولذلك فإن حمّى بيانات الموقع لا تزال مستمرة. ويقدّر ماكينسي القيمة السوقية لبيانات موقعك بأكثر من 100 مليار دولار ستعود على صناعات البيع بالتجزئة ووسائل الإعلام والاتصالات على مدى السنوات العشر القادمة.

ترتبط الـ "أين" بعددٍ من التقنيات، بهوائي هاتفك الذي يعمل بنظام تحديد المواقع العالمي وبالتقسيم الثلاثي لموقع هاتفك وبالمسافة بين أبراج الإشارة، وحتى بشبكات الإنترنت التي تتصل بها. وقد أصبحت بيانات الموقع هذه تضاف وبشكلٍ متزايد إلى المزيد والمزيد من تعاملاتك على الإنترنت في ما يُدعى ملف البيانات الواصفة، وهي بيانات تلخص أو تصف معلومات أخرى. فعلى سبيل المثال، عندما يلتقط الناس صوراً باستخدام

هواتفهم النقالة، فإن البيانات المتعلقة بأماكنهم، أي معلومات الموقع الجغرافي وخط الطول وخط العرض وغيرها من البيانات، غالباً ما تُوضع في ملفات الصور الناتجة. وعندما تقوم بتحميل هذه الصور والفيديوهات على مواقع مثل قائمة كريغ وفليكر ويوتيوب وفايسبوك وغيرها من مئات الخدمات، فإن هذه البيانات الفاضحة للأماكن قد تنتقل مع الملف الأصلي. وقد يكون الاهتمام بموقعك والسؤال عنه أمراً منطقياً بالنسبة لبعض التطبيقات، مثل خرائط غوغل أو أدوات الملاحة باستخدام نظام تحديد المواقع العالمي. لكن حصول البعض الآخر على بيانات الموقع يمثل طريقة أخرى يبيع من خلالها صانعو التطبيقات بياناتك بسعرٍ عالٍ.

تستخدم منشوراتك على فايسبوك وتغريداتك وعمليات البحث التي تجريها في موقع ييلب بيانات الموقع. علاوةً على ذلك، ثمة عدد متزايد من الشركات الناشئة التي تقدم خدمات معتمدة على الموقع تقوم بإقحام سؤال "الأين" في كل شيء، من التسوق وحتى العقارات. ولعل أحد أسرع الأسواق نمواً في مجال تحديد الموقع هي تلك التي تنطوي على الرومانسية والحب، وخاصة "حب" المؤقت لفترة محدّدة. إذ تم تحميل تطبيقات مثل تيندر وغريندر ملايين المرات، وهي قد تكون المسؤولة عن أكثر من خمسين مليون علاقة عابرة، وفقاً للمدير التنفيذي لتيندر. آه، تطبيقات الحب... إنها شيءٌ متعدد الامتيازات.

لكن مع كل هذه الفوائد المحتملة لهذه الدفعات الجديدة من بيانات الموقع، تبرز أيضاً مخاطر جديدة. ففي عام 2012 أطلقت شركة روسية تطبيقاً سمته الفتيات من حولي (Girls Around Me)، وتم قبوله وإدراجه في متجري أبل وغوغل للتطبيقات. وكان هذا التطبيق يستغل ما تنشره النساء عبر خدمات مثل الفايسبوك والفورسكوير من المنشورات العامة وتحديثات الحالات والصور وعمليات

تسجيل الدخول المرفقة ببيانات واصفة متعلقة بالموقع. فعندما يقوم مستخدم بتشغيل تطبيق "الفتيات من حولي" على هاتفه، لا يبقى عليه سوى الضغط على زر واحد لتظهر أمامه خريطة تفاعلية تظهر عليها أوجه فتيات موجودات في الجوار مع تحديد موقعهن بدقة. وباستخدام خاصية الرادار الموجودة في هذا التطبيق، يمكن لأي شخص أن يحدد مواقع هذه الفتيات وأن يرى حساباتهن على الفايسبوك.

على سبيل المثال، إذا استخدم رجل تطبيق الفتيات من حولي، ورأى أن امرأة جذابة قد سجلت دخولها توًّا من مقهى ستاربوكس قريب، فيمكنه ملاحقتها والدخول إلى حسابها على الفايسبوك ورؤية المدرسة أو الكلية التي كانت تدرس فيها، وليعلم أنها أمضت مؤخراً عطلتها في لاس فيغاس وليكتشف اسمي والديها ومشروباتها المفضلة، وحقيقة أنها في الصباح الباكر من ذلك اليوم شاهدت برنامج "البرتقالي هو الأسود الجديد" على موقع نيتفليكس. مسلحاً بتلك المعلومات، يمكن لهذا الرجل الغريب، مفتعلاً العفوية، أن يتجه إلى تلك المرأة وهي تنتظر دورها لتطلب وجبتها اليومية واللاتيه بحليب الصويا، ليتجاذب معها أطراف الحديث ويروي لها كم يحب فيغاس وبرنامج "البرتقالي هو الأسود الجديد". إنها أداة مفيدة جداً للحصول على موعد غرامي، لكنها مفيدة أيضاً للمطاردين والمغتصبين الباحثين عن نساء على مزاجهم.

أما بالنسبة للمعلنين، فإن كلمة "أين" لا تعني فقط مكانك الحالي، بل أيضاً أين كنت البارحة وقبل شهر وأين تحب أن تكون غداً. فسجلات الموقع تبين بالتفصيل المدة التي تقضيها في متجر ميسي مقارنة بمحل بيست بيي، ولهذه التحركات تبعات تفضح المزيد بعد. ففي عالم الإعلان الحديث القائم على بيانات الموقع، عندما تصطحب امرأة هاتفها الذكي بما يحويه من تطبيقات إلى عيادة الطبيب، يقوم النظام الإعلاني البيئي للهاتف

بتخزين سجل بيانات على درجة من الأهمية. لكن عندما تدخل المرأة نفسها محل "بيبيز آر يوز" بعد ثلاثة أسابيع، يصبح بالإمكان الكشف عن حقيقة أعمق بكثير. فعندما يتم جمع البيانات المتعلقة بمكانك طوال الوقت، يصبح بإمكان المعلنين معرفة ما إذا كنت تذهب إلى الكنيسة أم إلى الكنيس، وما إذا كنت تتدرب في قاعة رياضية أم تحتسي الشراب في البار، تراجع طبيبك النفسي أم تخون زوجتك. لكن من هم بالضبط هؤلاء الناس الذين يجمعون كل هذه المعلومات، وما هو مقدار هذه المعلومات التي بحوزتهم، وما الذي يفعلونه بها؟ كما ستكتشف بنفسك بعد قليل، فإن مقادير هذه البيانات هائلة وتزداد بمعدل أسّي وسيكون لها استخدامات لم نبدأ بعد، لا نحن ولا هم، بالتكهن بها.

الفصل الخامس
اقتصاد الرقابة

في الحقبة الرقمية، يجب أن تتمتع الخصوصية بالأولوية القصوى. هل أنا واهم، أم فجور رقابة الستار السري قد تجاوز حده؟

آل غور

كان لاي فان بريان يتطلع إلى اليوم الذي سيقوم فيه بأول عطلة أميركية له. فقبل بضعة أيام على رحلته إلى لوس أنجلوس، دخل البريطاني البالغ من العمر ستةً وعشرين عاماً إلى تويتر وسأل صديقة له ما إذا كان "لديها وقت هذا الأسبوع لبعض الثرثرة قبل أن يذهب ويدمّر أميركا". كان من الممكن لأي من مواطنيه البريطانيين في العشرينيات من العمر أن يفهم بسهولة ما يقصده باستخدام كلمة "يدمّر"، فهي تعني في العامية البريطانية "الاحتفال حتى الانهيار". لكن ما كان ينتظر فان بريان عند وصوله إلى أميركا لم يكن له علاقة كبيرة بالاحتفال.

فقد كان قسم الأمن المحلي يراقب الوسائط الاجتماعية عن كثب تحسباً لأية تهديدات ضد أميركا، وقد أصبح فان بريان الآن في قبضتهم. فلدى وصوله إلى لوس أنجلوس، كان في استقباله، هو ومرافقته إيميلي بونتينغ البالغة من العمر 24 عاماً، عملاء مسلحون من هيئة حماية الجمارك والحدود، اقتادوهما مقيّدين إلى زنزانة تقاسماها مع من بدوا كأنهم تجار مخدرات مكسيكيون لمدة اثنتي عشرة ساعة. وعلى الرغم من محاولات الاثنين شرح المعنى الدارج لكلمة "تدمير"، فإن المسؤولين الأميركيين لم يفهموا ما يقصدان. وقام العملاء الفدراليون مراراً بتفتيش الاثنين وحقائبهما بحثاً، من غير شرح، عن مجارف. إلا أن تغريدة أخرى كانت قد أتت على ذكر "نكش مارلين مانرو من قبرها"، وهي تذكير غير مباشر بحلقة من مسلسل "فاميلي غاي" الكرتوني، كانت قد أثارت بدورها إنذاراً جدياً

لدى أمن الداخل، الذي خشي على بقايا النجمة الراحلة. وبعد ليلة مزعجة قضياها في زنزانتين منعزلتين، اجتمع فان بريان وبونتينغ من جديد، ليتم رميهما مباشرة في طائرة عائدة إلى المملكة المتحدة. فقد منع الاثنان دخول الولايات المتحدة وتم ترحيلهما إلى بريطانيا. وفي نهاية المطاف كان ما دُمّر بالفعل هو تأشيرات الدخول والإجازة.

كنت تعتقد أن القراصنة أشرار؟ ماذا ستقول عن سماسرة البيانات؟

أكسيوم، إبسيلون، داتالوجيكس، رابليف، ريد إلسيفيَر، بلو كاي، سبوكيو وفلارّي، معظمنا لم يسمع في حياته بهذه الشركات، لكنها، مع شركات أخرى، مسؤولة عن صناعة مراقبة البيانات التي تتطور بسرعة وتصل قيمتها الحالية إلى 156 مليار دولار في العام. فبينما صُدِم المواطنون في أنحاء العالم بحجم ومدى عمليات المراقبة التي كانت وكالة الأمن القومي تمارسها، والتي كشف عنها إدوارد سنودن، من الهام أن نشير إلى أن العوائد السنوية البالغة 156 مليار دولار التي تحققها صناعة سمسرة البيانات، توازي ضعفي ميزانية الاستخبارات في الحكومة الأميركية. وتأتي البنى التحتية والأدوات والتقنيات التي تستخدمها هذه الشركات بالكامل تقريباً من القطاع الخاص، إلا أن العمق الذي يمكنها الوصول إليه في حياة المواطنين كفيل بإثارة الغيرة والحسد لدى أي وكالة استخبارات.

يحصل سماسرة البيانات على معلوماتهم من مزودي خدمة الإنترنت ومصدِري البطاقات الائتمانية وشركات الهواتف النقالة والمصارف ومكاتب الإقراض والصيدليات، ومراكز العربات ومتاجر البقالة، إضافة إلى نشاطاتنا على الإنترنت. فجميع البيانات التي نتخلى عنها يومياً بالمجان على الشبكات الاجتماعية، أي كل "إعجاب" وكل "نعرة" وكل تغريدة، يتم وسمها وإعطاؤها رمزاً جغرافياً وترتيبها ليعاد بيعها للمعلنين والمسوقين. وحتى تجار التجزئة، المنتمون إلى عالم قديم، باتوا مدركين لتوفر مصدر

دخل إضافي هائل لديهم، هو بيانات زبائنهم، قد يكون أوفر من المنتج أو الخدمة الفعلية التي يبيعونها. فالشركات تتهافت على التربّح من قناة العائدات الجديدة هذه لتحويل بنية البيانات التحتية لديها من مركز كلفة إلى مركز ربح. ومع أن مكاتب الإقراض، كإكسبيريان وترانس يونيون وإيكيفاكس، موجودة بيننا منذ عقود، فإن نمط حياتنا الجديد الذي تتزايد فيه الاتصالات عبر الإنترنت، يسمح لشركات جديدة بالتقاط أية قطرة بيانات جديدة متعلقة بحياتنا، الأمر الذي كان في السابق مستحيلاً لا يمكن تخيله.

تشغّل شركة واحدة، هي شركة أكسيوم في ليتل روك بأركانساس، أكثر من 23 ألف مخدّم حاسوبي "تجمع وتقارن وتحلل" أكثر من 50 تريليون مناقلة بيانات مستقلة كل عام. تحتوي قواعد بيانات أكسيوم على معلومات عن ستة وتسعين بالمئة من البيوت الأميركية، وقد بنت الشركة ملفات لأكثر من ' مليون مستهلك في أنحاء العالم. ويحتوي كل من هذه الملفات على أكثر من ألف وخمسمئة تفصيل لكل فرد، كالعِرْق والجنس ورقم الهاتف ونوع السيارة التي يقودها، ومستوى التعليم، وعدد الأولاد، ومساحة المنزل، وحجم الميزانية، وآخر المشتريات والعمر والطول والوزن والحالة الاجتماعية، والمشكلات الصحية، والمهنة، واليسراوية، إضافة إلى الحيوان المنزلي المقتنى وفصيلته.

تهدف أكسيوم وغيرها من سماسرة البيانات إلى تقديم ما يسمى مثلاً "الاستهداف السلوكي"، "الاستهداف التنبؤي"، "الرؤى السلوكية الرئيسية الاحتكارية" التي تتناول شخصيتك وحياتك. يعني ذلك، إذا ما أردنا التبسيط، محاولة فهمك بدقة فائقة تسمح لسماسرة البيانات ببيع المعلومات التي يجمّعونها بأعلى سعر ممكن للمعلنين والمسوقين والشركات الأخرى التي تحتاج هذه البيانات في عمليات صنع القرار. فعرض إعلان

بامبرز على طالب جامعة في التاسعة عشرة سيكون على الأغلب مضيعة لميزانية التسويق التنفيذية، لكن عرض المعلومات نفسها على ربة منزل حامل في الثانية والثلاثين قد يقود إلى مئات الدولارات من المبيعات. ولتحقيق الحد الأقصى لقيمة الذكاء الرقمي الذي يعملون على جمعه، لا ينفك سماسرة البيانات يقسموننا إلى فئات فرعية وملفات أكثر تحديداً. إنه عالم رقابة البيانات.

تبيع أكسيوم ملفات الزبائن التي لديها إلى اثنتي عشرة من كبرى الشركات المصدرة للبطاقات الائتمانية، وسبعة من أكبر بنوك المستهلك، وثماني من كبرى شركات الاتصالات وتسع من أكبر شركات التأمين. "تمنحك أكسيوم رمزاً مؤلفاً من 13 خانة وتضعك ضمن أحد "العناقيد" اعتماداً على سلوكك وعلى بياناتك البشرية". ففي العنقود 38 على سبيل المثال، "نجد الأشخاص الأميل لأن يكونوا أفريقيين - أميركيين أو من أصول أميركية لاتينية، وأهالي عاملين لمراهقين، والطبقة الوسطى الدنيا وزبائن محالّ التخفيضات". أما من هم في العنقود 48، فهم أميل لأن يكونوا "من أصول قوقازية مع تعليم ثانوي، ريفيين ويميلون إلى العائلة يهوون الصيد وصيد السمك ومشاهدة ناسكار". وتباع هذه البيانات أيضاً إلى سماسرة آخرين يمثلون طرفاً ثالثاً يطبقون عليها بدورهم خوارزمياتهم الخاصة، ليزيدوا من معايرة مجموعات البيانات لإنشاء قوائم فئات خاصة بهم مثل "العائلات المسيحية"، و"المقامرين المتحمسين على الشبكة"، و"عديمي الحركة" و"من أصول أميركية لاتينية ويردّون في يوم السداد".

قد يتلقى أولئك المصنفون تحت "عائلات مسيحية" إعلانات لنسخ الإنجيل أو لموقع اللقاء المسيحي، بينما يتم استهداف المقامرين، أو أولئك الذين تحكم خوارزمية ما بأنهم "عديمو الحركة"، بإعلانات لمقرضين مغمورين أو لبرامج إيفاء ديون. ومع أن فئات مثل العائلات المسيحية أو

"الإناث الجامعيات من أصول أميركية لاتينية"، قد تبدو غير مزعجة، فإن بعض سماسرة البيانات يبيعون قوائم أكثر إزعاجاً بكثير إلى المعلنين وإلى أطراف أخرى غير معروفة. إذ يعرض بعض السماسرة قوائم بالمعمرين المصابين بالخرف أو أولئك الذين يتعايشون مع مرض الإيدز، بينما عرضت شركة أخرى، هي ميدبيز200، بالمزاد قوائمها التي تحتوي كلاً من ضحايا العنف المحلي وضحايا الاغتصاب.

برز مدى وعمق عمليات جمع البيانات التجارية واقتصاد الرقابة في بداية عام 2014 عندما تلقى أب مكلوم في ليندنهورست بولاية إلينويس، منشوراً ترويجياً وصله بالبريد من متاجر أوفيس ماكس للتجزئة، معنوناً بعبارة "مايك سيي، قضت ابنته في حادث سيارة"، يليه عنوان منزل الرجل. وقد وجد المرسل الرجل المطلوب بالفعل، فقد كانت ابنة سيي، وكان عمرها سبعة عشر عاماً، قد قضت في حادث تصادم سيارة مع صديقها الحميم قبل ذلك بسنة. وعندما اتصل سيي بأوفيس ماكس ليشتكي ما حدث، رفض المدير تصديقه وتجاهل دعواه قائلاً إنها "مستحيلة". ولم تعترف الشركة بالخطأ إلى أن نشرها مراسل محلي لشبكة إن.بي.سي لتقول عندها إنه "نتيجة قائمة مراسلة مستأجرة من قبل مزود آخر". وفي النهاية، تلقى سيي مكالمة هاتفية من موظف صغير في أوفيس ماكس اعتذر عن الحادثة، لكنه رفض طلب سيي المتكرر بتسمية سمسار البيانات المسؤول عن الحادث. كما لم يقبل الموظف التصريح عما إذا كانت الشركة تحتفظ ببيانات مشابهة حول زبائن آخرين محتملين. من الواضح أن قصة سيي مزعجة، خصوصاً أنه ليس زبوناً دائماً لدى أوفيس ماكس، بل كان يشتري من حين لآخر ورقاً لطابعته من هناك.

تطرح هذه الحادثة بعض الأسئلة الجدية حول صناعة سمسرة البيانات. فأية بيانات مفصلة تمتلكها أوفيس ماكس بعد عن حياة زبائنها على سبيل

المثال؟ وسمسار البيانات الذي باع هذه المعلومات أساساً، ماذا تخفي قواعد بياناته بعد عنك وعن عائلتك؟ أخ كحولي؟ أم فصامية؟ ابنة في الثالثة عشرة لديها اضطرابات في الطعام؟ ما هي التشريعات القائمة التي يمكنها وضع حد لما يمكن لسماسرة البيانات أن يفعلوه بهذه المعلومات، وماذا يمكنك أن تفعل إذا كانت المعلومات المتوفرة لديهم عنك غير صحيحة؟ لكن ليس من الصعب إدراك أن التشريعات تكاد تكون معدومة. فالأمر أشبه بحبكة رواية فرانز كافكا "المحاكمة"، التي يتم فيها القبض على رجل دون إعلامه بالسبب، ليعلم في ما بعد أن محكمة سرية تحتفظ بملف سري عنه لا يحق له الاطلاع عليه. فسماسرة البيانات المعاصرون، على خلاف وكالات التقارير الائتمانية، يعملون من دون أية تشريعات من قبل الحكومة تقريباً. فما من قوانين، مثل قانون التقارير الائتمانية العادلة، يفرض عليهم الحفاظ على خصوصية الزبون وتصحيح أية أخطاء في المعلومات، بل الكشف عن المعلومات المتوفرة عنك وعن عائلتك في أنظمتهم.

نتيجة للتجربة التي مر بها سيي والآلاف من أمثاله، بدأ الكونغرس، بقيادة السيناتور جي روكفيلر من فيرجينيا الغربية، ولجنة التجارة الفدرالية ومكتب الحماية المالية للمستهلك، بالتحقيق في طبيعة ومدى صناعة سمسرة البيانات التي تدر المليارات من الدولارات. لكن أية تغييرات تشريعية قد تكون ذات معنى ستواجه معارضة شرسة من سماسرة البيانات الذين تتوفر لديهم الأموال اللازمة وأكثر. علاوة على ذلك، ما إن تخرج البيانات، حتى يصبح من المستحيل عملياً "إعادة معجون الأسنان إلى الأنبوب". وتستمر شركة أكسيوم وغيرها في تكديس المعلومات حولك في هذه الأثناء. ففي نهاية عام 2013، أعلن رئيس مجلس إدارة أكسيوم، سكوت هاو، بفخر أن شركته قد جمعت حوالى 1.1 مليار مفردة بيانات من

المتصفحات من طرف ثالث وتعرفت أجهزة أكثر من 200 مليون زبون أنشأت لهم ملفات خاصة. "سيشمل مجالنا الرقمي قريباً كل مستخدم إنترنت في الولايات المتحدة تقريباً"، على حد تأكيده.

عبر التنقيب في قواعد البيانات العمومية وتجميع هذه المعارف مع المعلومات الشخصية التي يشاركها الناس، عمداً أم من غير عمد، عن أنفسهم وأصدقائهم وعائلاتهم على الوسائط الاجتماعية، بات بمقدور شركات مثل أكسيوم أن تنشر أشمل نظام مراقبة استخباري ظهر إلى الوجود وإقحامه في حياة كل أميركي حي اليوم. يمثل هذا الإنجاز التقاني "العرف الجديد" في مجتمع رقابة البيانات الذي نعيش فيه، وهو جزء مما نعته نائب الرئيس السابق آل غور ب- "اقتصاد المطارِدين" في خطابه في مهرجان "جنوب وجنوب غرب" التفاعلي في أوستين بولاية تكساس.

وكان غور محقاً، فما بات واضحاً اليوم هو أن الرقابة هي النموذج التجاري الخاص بالإنترنت. فبإمكانك إنشاء حساب "مجاني" على مواقع مثل سنابتشات وفايسبوك وغوغل ولينكيدإن وفورسكوير وبيشنتس.لايك.مي، وتحميل التطبيقات المجانية مثل الطيور الغاضبة وكاندي كراش ساغا و"كلمات مع الأصدقاء" و"فواكه النينجا"، لكنك بالمقابل، سواءٌ قصدت ذلك أو لا، توافق على السماح لهذه الشركات بتتبع جميع تحركاتك وتجميعها ومقاطعتها وبيعها إلى أكبر عدد ممكن من الزبائن وبأعلى سعر، لا تردعها عن ذلك تشريعات أو قيود ذاتية أو أخلاقية. إلا أن قلة قليلة تتوقف وتتساءل عمن يمكنه الوصول إلى هذه البيانات المبعثرة وكيف يمكن أن يتم استخدامها ضدنا. فرقابة البيانات هي "آخر صيحة"، واستخداماتها وقدراتها وطاقاتها توشك على الانفجار بطرق لا يمكن سوى لقلة من المستهلكين والحكومات والتقانيين تخيلها.

إخضاعك للتحليل

بات كلّ منا يخلف وراءه أثراً من المخلفات الرقمية خلال اليوم في سيل مستمر من السجلات الهاتفية والرسائل النصية ومدخلات تاريخ المتصفح والبيانات الجغرافية ورسائل البريد الإلكترونية التي ستبقى إلى الأبد. ويسمح تحليل هذه المعلومات للشركات بالعثور على الزبائن المحتملين بدرجات دقة أعلى بكثير مع تحقيق نتائج أعلى بكثير مما كان ممكناً ذات يوم. ولنقل على سبيل المثال أنك ترغب في اصطحاب عائلتك في إجازة إلى شاطئ ميامي. ستقوم بالبحث عن رحلات طيران على موقع كاياك، وبعدها تدخل إلى متجر إلكتروني وتشتري ملابس سباحة ببطاقتك الائتمانية. إن الجمع بين البيانات القادمة من عملية شراء ملابس السباحة وبين بيانات متصفحك يعزز احتمال بحثك عن غرفة فندق تحجزها في ميامي. ونتيجة لهذا التحليل السلوكي، تتجمع لديك بيانات ذات قيمة قابلة للحساب يمكنك تقديمها إلى الفنادق في ميامي، والتي سيزايد بعضها على بعض، وبالزمن الحقيقي، عبر تقديم الإعلانات التي تصلك بمحتويات وعروض في غاية الصلة بحاجتك بناءً على سلوكك المزمع.

غوغل ناو، الذي يعد بتقديم "المعلومات الصحيحة تماماً في الوقت المناسب تماماً"، هو مثال آخر على التحليل العميق الذي يطبق على قواعد بيانات ضخمة. حيث يقدم تطبيق غوغل ناو للزبائن معلومات مريحة رائعة تساعدهم في التقاط جميع البيانات التي تدور غير مرئية من حولهم والاستفادة منها. فحال موافقة المستخدمين على اتفاقية الخدمة، يعرض عليهم غوغل ناو أوقات توفر أصدقائهم في الجوار، وتحذيرات مرورية، ويحدد أسرع طريق للقيادة إلى المنزل وإلى العمل، ويقدم تلقائياً تقرير الطقس الصباحي، ويحتفظ بأخبار الفرق الرياضية المفضلة ويحدث نتائج المباريات بالزمن الحقيقي. يستطيع غوغل ناو إخبارك بتأجيل رحلة طائرتك وتغيير البوابة في المطار ويعرض عليك رحلات طيران بديلة في حال

توفرها. ولأن غوغل ناو يعلم أماكن جميع مواعيدك ويراقب بالزمن الحقيقي مواقع الاختناقات المرورية على جميع المسارات التي قد تسلكها، فإن التطبيق سينبهك في موقعك وينصحك بالمغادرة مبكراً إذا كنت تريد أن تصل إلى موعدك القادم في الوقت المناسب. وباستخدام تقنية تعرف بـ "السياج الجغرافي"، يستطيع غوغل ناو تحليل قائمة مهامك ومقارنتها بموقعك الذي يتم تتبّعه باستمرار، لكي ينبهك عندما تمر بالقرب من متجر بقالة ليذكرك بأن عليك أن تشتري الحليب. للتمتع بجميع الميزات المعلوماتية وأسباب الراحة هذه، ليس عليك سوى السماح لتطبيق غوغل ناو بالوصول إلى جميع آثارك الرقمية، بما فيها صندوق الرسائل الواردة في بريد جيميل الإلكتروني، وعمليات البحث على الوب وحجوزات الفنادق ورحلات الطيران وقوائم المعارف وأعياد ميلاد الأصدقاء وحجوزات المطاعم والمواعيد المسجلة في التقويم إضافة إلى موقعك الفيزيائي في كل لحظة عبر نظام تحديد الموقع في هاتفك النقال. ومن هذا الكم الهائل من البيانات، يستطيع غوغل (وغيره) إعادة تشكيل ما يسميه محللو الذكاء "نموذج حياتك"، عبر معرفة وتخطيط موقعك الفيزيائي عبر الوقت إضافة إلى ما تقوم به ومع من. إنه مريح إلى حد مرعب!

لكن ماذا يمكن لغوغل أو لأي شركة أخرى تتوصل إلى نموذج حياتك أن تستخلص؟ لنقل على سبيل المثال إن هاتفك النقال يبقى على طاولة السرير نفسها، التي تضع عليها زوجتك هاتفها ست ليالٍ في الأسبوع. من المنطقي أن يستخلص من هذه البيانات أن مالكي الهاتفين الخلويين يعيشان معاً وأنهما على الأرجح ينامان معاً. لكن ماذا إذا كان هاتفك النقال ذات ليلة من الأسبوع على طاولة سرير ما بجوار هاتف امرأة أخرى؟ ما الذي يعنيه ذلك لغوغل وغيره حول إخلاصك؟ من شأن تحليل بيانات الموقع الخاصة بك وتلك العائدة إلى هواتف (وتطبيقات) تحيط بك أن يعطي تقريباً

ممتازاً لمتانة وقوة شبكاتك الاجتماعية الشخصية والمهنية. وعندما تتم دراسة البيانات الصادرة عنك على المدى الطويل، يصبح بالإمكان الخروج بالكثير من الخلاصات الأخرى حول حياتك. وقد درس الباحثون في المملكة المتحدة على سبيل المثال مواقع مستخدمي الهواتف النقالة في الماضي، فتمكنوا عبر تطبيق تقانات بسيطة لتحليل البيانات من معرفة المكان الذي سيكون فيه أحد المستخدمين في الوقت نفسه من اليوم التالي في نطاق قطره عشرون متراً، وهي أداة مفيدة جداً لكل من المعلنين والمطاردين. فهاتفك يعلم اليوم ليس فقط أين كنت، بل أين ستكون أيضاً.

من شأن تحليل شبكتك الاجتماعية وأفرادها أيضاً أن يكشف عن الكثير عن حياتك وميولك السياسية والجنسية، كما تبين الدراسة التي أجراها معهد ماساتشوستس للتقانة. ففي عملية تحليل تعرف باسم غيدار، درس الباحثون ملفات الفايسبوك لألف وخمسمئة طالب في الجامعة، كان منهم من ترك حقل التوجه الجنسي فارغاً أو قال إنه يميل إلى الجنس الآخر. وبناء على أبحاث سابقة بينت أن الرجال غير الأسوياء أميَل لأن يكون لديهم أصدقاء مثلهم (وما من مفاجأة في ذلك)، صاغ الباحثون معياراً بيانياً قيّماً لاستخدامه في مراجعة علاقات الصداقة بين طلاب العينة. وكانت النتيجة هي قدرة الباحثين على التنبؤ بدقة بلغت 78 بالمئة بما إذا كان طالب ما سوياً أم لا. وكان ثمة ما لا يقل عن عشرة أفراد لم يتم التعرف عليهم قبل ذلك بأنهم غير أسوياء، لكن الخوارزمية صنفتهم كذلك، لتتأكد نتيجة التحليل عبر مقابلات شخصية معهم. وإذا كانت هذه النتائج قد لا تثير قلقاً في بيئات متحررة مثل كامبريدج وماساتشوستس، فإنها قد تصبح إشكالية في البلدان الستة والسبعين التي تجرّم المثلية الجنسية، كالسودان وإيران واليمن ونيجيريا، حيث قد تصل عقوبة هذا "الإثم" إلى الرجم. وقد بينت دراسة تناولت 58 ألف مستخدم على الفايسبوك ونشرتها الأكاديمية

الوطنية للعلوم أن دراسة تعبيرات "الإعجاب" وحدها كفيلة بتحديد تفاصيل حميمية وخصائل شخصية بدقة مفاجئة. إذ تمكنت الدراسة الرصينة التي أجريت بالتنسيق مع جامعة كامبريدج، من التنبؤ بما إذا كان مستوى ذكاء المستخدم عالياً أم منخفضاً وما إذا كان مستقراً عاطفياً وما إذا كان من أسرة مفككة. فمشكلة البيانات التي تتسرب منا هي أن بإمكان الآخرين، كما تبين العديد من الحالات، أن يجمعوا هذا الفتات الرقمي ويفسروه دون معرفتنا بطرق قد تسبب لنا الأذية.

لكن ليس لدي ما أخفيه

في شهر كانون الثاني عام 2009 حين سألت ماريا بارتيبومو من شبكة سي.إن.بي.سي رئيس مجلس إدارة غوغل إريك شميدت، عن المخاوف المتعلقة بالخصوصية الناجمة عن زيادة عمليات التتبع التي تجريها غوغل على الزبائن، جاء جواب شميدت الشهير "إذا كان لديك شيء لا تريدين لأحد أن يعلم به، ربما كان عليك ألا تقومي به أساساً". فشميدت وغيره يغلقون ملف الخصوصية بالقول إنك إذا لم تكن قد فعلت شيئاً خطأً فليس عليك أن تخشى أن يعلم الناس (أي الشركات والحكومات والجيران) بالأمر.

وتردد صدى هذا التصريح من مارك زوكربيرغ رئيس مجلس إدارة فايسبوك الذي دافع عن أن "الخصوصية لم تعد المعيار الاجتماعي". لكن بينما لم تعد الخصوصية هي المعيار الاجتماعي، على الأقل بالنسبة للعامة، في حياته الخاصة، يبدو أن السيد زوكربيرغ يكنّ بالفعل بعض التقدير للخصوصية. ففي أواخر عام 2013، تم الكشف عن أن رئيس إدارة الفايسبوك قد أنفق 30 مليون دولار لشراء أربعة منازل تحيط بملكيته لكي يضمن أن تبقى خصوصيته في منأى عن المتطفلين والمزعجين.

واقترحت مدير العمليات في فايسبوك، شيرلي ساندبرغ، بدوره أن إصرارك على أية حقوق في الخصوصية يقع في تناقض مع "أصالة الهوية". وتنوه

ساندبرغ إلى أن "إثبات صحة الهوية سيصبح أكثر أهمية بعد في السنوات القادمة... وأجل، سيتطلب هذا التحول في أهمية الهوية إلى الاعتياد، وستتعالى الصرخات لضياع الخصوصية". لا بد أنه من دواعي سرور شميدت وزوكربيرغ وساندبرغ أن تكون هذه "التغيرات الطبيعية" في المعايير الاجتماعية متناسقة مع خطط الأرباح والخسائر الشخصية والمهنية، والتي تنتفع مباشرة من الأموال الناتجة عنك وعن جبال المعلومات التي تسربها بأقصى حد ممكن، نتيجة اتفاقية خدمتهم المعدة من جانب واحد.

لكن قول "ليس لدي ما أخفيه" هو أسوأ طريقة نتناول فيها مجتمع رقابة البيانات الجديد الذي نعيش فيه. إنه تخيير خطأ في المقام الأول، فإما أن نقبل بالرقابة المطلقة أو أننا مجرمون وموضع شبهة عن جدارة. فإذا كان أنصار "لا شيء لأخفيه" يعنون ما يقولون، فمن المنطقي أنهم لن يعترضوا إذا قمنا بتصويرهم وهم يضاجعون زوجاتهم ونشرنا عوائدهم الضريبية على الإنترنت وعرضنا نقلاً مباشراً من حماماتهم على شاشة عرض أمام حشد من الجماهير، إذ لا شيء لديهم يخفونه في النهاية. لكن الحقيقة هي أن لكل منا لحظات خصوصية معينة في الحياة، تستمد استثنائيتها من الحدود المقامة على من يطلعون على تفاصيلها الحميمة.

أما أولئك الذين يتوهمون أنه لا شيء لديهم يخفونه، فقد يحتاجون درساً مناسباً يبين لهم ما الذي قد يخشونه، فكل منا لديه تفاصيل في حياته يفضل عدم مشاركتها مع غيره. فتصور لو كان لدى غوغل وسكايب ومشغلات الهاتف النقال وأي من الوكالات الحكومية سجلات تبين من اتصل بعيادة إجهاض أو بخط مساعدة في مواضيع الانتحار أو بخط مساعدة الكحوليين مغفل الهوية، أو لو كان مجمعو البيانات يعلمون مَن بحثَ عن "مشجعات داعرات"، أو "فياغرا" أو "بروزاك" من أي من الأجهزة الإلكترونية. ومع أن جميع هذه النشاطات قانونية تماماً، فما من شك في أن

لها وقعها في مجتمعنا إذا ما خرجت إلى الملأ.

إذا تمعنا في حيازة غوغل وفايسبوك وحدهما لعدة مئات من التيرابايتات من البيانات حول مستخدميهم مخزنة إلى الأبد، ربما كان السؤال الذي يجدر بنا طرحه ليس "من لديه شيء يخفيه"، بل ما الذي نود له أن يبقى خصوصياً في المستقبل. لو كان فايسبوك موجوداً عام 1950، كيف كان التاريخ سيحكم اليوم على مزحة سمجة من ذلك الوقت؟ أية جرائم قد تحاكم بها في المستقبل دون أن تكون على علم بأنك تخرق القانون أساساً؟ هل كنت تقطع الحدود بين نيو جيرسي وديلاوير لكي توفر الضرائب عند شراء ملابس المدرسة لأبنائك؟ لقد تم توثيق تهربك الضريبي بواسطة هاتفك النقال وإيصالات بطاقة الائتمان. أما تلك الصورة على موقع تويتبيك لغداء العائلة، والتي يظهر فيها ابنك في العشرين هو يحتسي النبيذ، إنها دليل على تقديم الكحول لقاصر. وعلى حد قول موكسي مارلينسبايك الباحث في مجال أمن الحاسب فإن "ثمة 27,000 صفحة من التشريعات الفدرالية" في الولايات المتحدة و"10,000 غيرها من التشريعات الإدارية. فلا بد أن لديك ما تخفيه، لكنك ببساطة لا تعلم".

مخاطر تحيق بالخصوصية ومفاجآت أخرى غير سارة

كما بينت تجارب مات هونان من مجلة ويريد ومايك سيي، الأب المكلوم، فإن بياناتنا الشخصية قد تنتهي في أيدي أولئك الذين لا نريد لهم أن يصلوا إلى مثل هذه المعلومات. فالجمع بين خلطة البيانات الاجتماعية وقواعد البيانات العمومية وبيانات المتصفحات والمواقع الجغرافية، قد يؤدي إلى نتائج غير متوقعة، بل ومؤذية. بعبارة أخرى، بياناتك تزداد خيانة لك. فهي تسري من نظام إلى آخر، من قاعدة بيانات إلى أخرى، تختفي وتتوزع بين الشبكات السحابية في أنحاء العالم، فتتم مشاركتها ومعالجتها وبيعها. لكن ما يعلمنا إياه العالم الحقيقي هو أن الخيانة كثيراً ما تقود إلى أمراض

اجتماعية وعواقب أخرى غير متوقعة.

في حادثة لا تختلف كثيراً عن زلّة أوفيس ماكس، علم رجل من مينيابوليس أن ابنته حامل، لكنها لم تكن من أخبره، بل علم بذلك من أحد متاجر تارغيت المحلية. وكان له هذا الاكتشاف حين بدأ المتجر يرسل إلى الفتاة، وكانت في الخامسة عشرة، قسائم لمنتجات لم تكن تتوافق مع اهتمامات الأب. فحمل الأب القسائم ورسالة من المتجر كانت موجهة لابنته وتوجه بها إلى المتجر ليستعلم من مديره. "ابنتي تلقت هذه الرسالة!... هي لا تزال في الثانوية، وأنتم ترسلون لها قسائم لملابس وأسرّة الرضّع؟ هل تحاولون تشجيع ابنتي على الحمل؟". وبعد بضعة أيام، اتصل الرجل بالمتجر منوهاً إلى أنه "كانت ثمة نشاطات في منزلي لم أكن على علم بها تماماً. ابنتي ستضع في آب. وأنا مدين لكم باعتذار". لكن كيف كان لمتجر تارغيت أن يعلم أن الابنة حامل؟ بواسطة خوارزمية التنبؤ بالحمل التي يستخدمها بالطبع، والتي تجمع تاريخ مشتريات الزبون بالكامل مع الإحصاءات السكانية التي يشتريها المتجر من سماسرة البيانات. ويقوم منطق متاجر تارغيت على أنها إذا استطاعت إيجاد النساء الحوامل قبل الثلث الثاني من الحمل واجتذابهنّ كزبونات لديها، فإنه ستضمن حصة الأسد، ليس من مشترياتهنّ من حفاضات الأطفال وأغطيتهم ومناديلهم وهم رضّع وحسب، بل من ألعابهم وألبستهم مع نمو الرضّع حتى يصلوا إلى سن المراهقة. وقد لاحظ الإحصائيون العاملون لدى تارغيت من خلال دراساتهم المعمّقة أن النساء المصنّفات في سجل الأمهات "يشترين كميات أكبر من مستحضرات الغسل غير المعطّرة في بداية الثلث الثاني، إضافة إلى مقويات الفيتامين كالكالسيوم والمغنيزيوم والزنك". وتمكن المتجر في نهاية المطاف من تحديد 25 منتجاً كفيلاً بتصنيف المتسوّقين وفق "مقياس احتمال الحمل". وعند تطبيق هذا النموذج على ملايين النساء في قاعدة

بيانات زبائن تارغيت، تم التعرف على الآلاف من النساء الحوامل قبل أن تتمكن أية شركة أخرى من إقامة هذا الربط. كانت متاجر تارغيت ومسوقو الشركة في غاية الحماسة لهذا الاكتشاف. أما من كان أقل حماساً فهو والد تلك الفتاة ذات الخمسة عشر ربيعاً في مينيابوليس، والذي علم بنبأ قدوم حفيده عبر قسيمة تجارية أتت بالبريد. فإذا ما تأملنا بعملية الاختراق التي تعرضت لها متاجر تارغيت عام 2014 والتي تسربت فيها البيانات المالية لـ 110 ملايين زبون، فأي ضمانات تتوفر للزبائن بعدم سرقة المجموعات الإضافية الهائلة من بيانات شخصية جداً والمحروسة في خزنات متاجر تارغيت؟ هل يمكن للزبائن ائتمان متاجر تارغيت أو أي من بائعي التجزئة الآخرين على كميات البيانات التي يجمعونها ويخزنونها ويحللونها؟ من الأرجح أن ذلك غير ممكن، وهنا تكمن المشكلة.

لا تتهدد بياناتنا الشخصية هجمات القراصنة وحدها، كما سيكتشف المزيد من الناس مع الوقت، بل تحليل البيانات الكبيرة أيضاً. فقد كانت معظم البيانات التي يتم جمعها في السابق منسيةً، لأن قدراتنا على جمع البيانات كانت تفوق قدراتنا على استخراج معاني ما نجمعه منها. لكن ذلك يتغير الآن، والبيانات التي نسرّبها على مواقع الوسائط الاجتماعية كالفايسبوك، تظهر مجدداً بطرق لم يكن أحد يتوقعها. ومن أولئك الذين تأثروا بهذا التغيير بوبي دونكان، وهي طالبة غير سوية جنسياً من جامعة تكساس في أوستين. فهي تنحدر من عائلة مسيحية متزمتة، وكانت تجهد في كتم توجهها الجنسي عن أبويها. وعندما بدأت تفهم نفسها فهماً أفضل، أخذت تشارك في عدد من مجموعات الطلاب في الجامعة، مثل كوير كورس، كوسيلة للالتقاء بغيرها من الطلاب الذين يشاركونها الميول نفسه في جامعتها. وعند انضمامها إلى المنظمة، رحب رئيس كوير كورس ببوبي بأن أضافها إلى صفحة مناقشات المجموعة على الفايسبوك، وكان بإمكانه فعل

ذلك من دون إذنها (فما من إعدادات في فايسبوك تمنع طرفاً ثالثاً من إضافتك إلى مجموعته). وعندها أرسل الموقع إشعاراً تلقائياً إلى جميع أصدقاء بوبي، بمن فيهم والدها، يعلمهم فيه بانضمامها إلى المجموعة. وبعد يومين على وصول الإشعار، كتب والد بوبي رداً على صفحته على الفايسبوك رسالة غاضبة. لقد فضح الفايسبوك بوبي دونكان وتسبب في تبرؤ والديها منها. وتعليقاً على الضرر الذي لحق بها، والذي لا يمكن إصلاحه، ردت بوبي، التي لم تكن في موقع تحسد عليه، "إنني ألقي اللوم على الفايسبوك... لا يجوز أن يختار آخرون لي ما يمكن للناس مشاهدته حولي".

عندما تكون منتجاً من منتجات الإنترنت وشركات الوسائط الاجتماعية، يكون التحدي الذي تواجهه هو أن البيانات التي تقدمها في سياق ما قد تستخدم في سياق آخر بطرق لا تتوقعها يكون لها عقبات لا يستهان بها. وهو ما ينطبق أيضاً على موقع التعارف المجاني "أوكيوبايد". فقد كان يطلب إلى المستخدمين الراغبين بالتعارف ملء استبيانات على الموقع، وكان معظمهم يفترض، عن خطأ، أن البيانات التي يقدمونها ستبقى ضمن نظام أوكيوبايد حصراً، وأنها ستستخدم حصراً بهدف إيجاد موعد غرامي مناسب. أجل، بالطبع! فللعثور على شخص متوافق تماماً مع طبيعة المستخدم على حد زعم الموقع، كان الموقع يطرح على المستخدمين كومة من الأسئلة التي تسبر أغوار شخصيتهم، كعدد شركائهم الجنسيين السابقين، وما إذا كانوا يؤيدون حق الإجهاض، وما إذا كان لديهم قطعة سلاح، وما إذا كانوا سينامون مع شخص ما في أول موعد غرامي معه، وما إذا كانوا يدخنون، وما إذا كانوا يحتسون الخمر أو يتعاطون المخدرات بشكل دوري وعن وتيرة تعاطيهم لها. كان هذا على الأقل ما كان المستخدمون يشاهدونه على شاشاتهم وهم يملأون ملفاتهم...

أما ما لم يكن يعرض عليهم، فهو حوالى خمسين شركة تُشارك أوكيوبايد

هذه المعلومات، من بينها شركات إعلان وسماسرة بيانات ومسوّقون. ولفهم مدى تسريب البيانات هذا، قام عشقان سلطاني، وهو متخصص في مجال الخصوصية الرقمية وكان يعمل في لجنة التجارة الفدرالية، بإنشاء حساب وهمي على الموقع. وباستخدام العديد من ملحقات المتصفحات المجانية المتعلقة بالخصوصية، مثل كوليجن وميتمبروكسي، تمكن سلطاني من اكتشاف أن الأجوبة التي يقدمها مستخدمو أوكيوبايد كانت تتم معالجتها وتحويلها إلى العشرات من سماسرة البيانات بالزمن الحقيقي. وحين أتمّ سلطاني ملفه التجريبي على أوكيوبايد، وصرح بأنه يتعاطى المخدرات بشكل دوري، لاحظ ملف بيانات للمتصفح (كوكي) يشارك المعلومات عن تعاطيه للمخدرات مع سمسار بيانات يدعى لوتيم. فعندما تعتقد أنك تملأ ملفاً سرياً "مجاناً" على خدمة تعارف، تكون في الواقع قد استُملِكت، وما يجري بالفعل هو أنك تقدم معلومات تفصيلية لم تكن لتشاركها مع أية شركة تسويق أو سمسار بيانات. إنها خدعة ماكرة، فما التعارف سوى "قصة الغلاف" التي تتستر على عمليات استخراج البيانات التي تجري بالجملة. وفي تحقيق لاحق تناول بحث سلطاني الذي أجرته الإذاعة الوطنية، رفض كل من موقع أوكيوبايد ولوتيم التعليق على الموضوع. وهي الحال دوماً في صناعة سمسرة البيانات العالمية غير المنظّمة. فمن هو المستعد لدفع المال لقاء أرشيف أوكيوبايد حول تعاطيك للمخدرات وتاريخك الجنسي؟ شركة تأمين، أو رب عمل مستقبلي، أو ربما الحكومة بعد مخالفة قيادة في حالة سكر كتبت لك في حزيران الفائت؟

حتى عندما "لا يكون لديك ما تخفيه"، ربما يعود بيان شبكتك الاجتماعية وموقعك الجغرافي ليزعجك، بل ليؤثر على حالتك المالية. فقد بدأت العديد من الشركات الناشئة العاملة في مجال التقانة، بدراسة طبيعة صداقاتك على شبكتك الاجتماعية للتحديد ما إذا كنت أهلاً للإقراض. ومن هذه

الشركات شركة ليندو التي تنظر ما إذا كنت صديقاً لشخص متخلف عن تسديد قروضه، وتدرس مدى تواصلك مع هذا الشخص. وقد تهبط أهليتك للإقراض بسبب أولئك الذين تصادقهم على الفايسبوك. وإذا كان على أصدقائك على غوغل بلس وبينتريست ديون ميتة، فمن الممكن أن يحدث ذلك معك أيضاً (وفقاً لآلهة البيانات الكبيرة). وقد يصبح الفايسبوك وكالة تقييم الاقتراض التالية خلفاً لوكالة فيكو عندما تتمكن مجمّعات البيانات من الاستفادة من كامل بياناتك الاجتماعية لتقييم استقرارك المالي. وكما اعتادت أمك أن تحذّرك: اختر أصدقاءك بحكمة.

الحقيقة هي أننا جميعاً نسهم في تلوثنا الرقمي بأنفسنا. فتماماً كما كان الناس في القرن العشرين لا يرون ضيراً في صب النفايات الصناعية في نهر أو في رمي القمامة في الشارع، نجدنا أيضاً غير قادرين على إدراك التبعات الطويلة المدى لأفعالنا الرقمية اليوم. والظروف القائمة حالياً تعود إلى إساءة فهمنا أساساً للصفقة التي أجريناها مع الخدمات الشبكية التي يزعم أنها "مجانية".

فتح صندوق باندورا الافتراضي

يشارك الناس أكثر أفكارهم وأسرارهم حميمية على الشبكة كأنهم في محادثة خاصة مع صديق موثوق. لكن ليت النظام القانوني يوافقهم في ذلك. ففي الولايات المتحدة تعتبر الشبكات الاجتماعية فضاءات عمومية لا خصوصية، وأية معلومات تتم مشاركتها عليها تخضع لما يسمى بمبدأ الطرف الثالث، والذي يعني، إذا ما أردنا التبسيط، أنه ما من سبب يدعو المستخدمين لتوقع الخصوصية في ما يتعلق بالبيانات التي يجمعها عنهم مزودو الخدمات (أي شركات الهواتف الخلوية ومزودي خدمات الإنترنت وشركات الكابلات ومواقع الوب).

وهذا الاستثناء الواضح من التعديل الرابع الذي يمنع الملاحقة والاعتقال

غير المبررين، يعني أن أية بيانات تقوم بنشرها على الشبكة بأية صيغة (وبغض النظر عن إعدادات الخصوصية التي تحددها)، وأية بيانات يتم جمعها من قبل طرف ثالث تتفق معه على علاقة تجارية، لا تعتبر بيانات خصوصية. كما لا ينطبق عليها التعريف الدستوري لـ "الأوراق الخاصة"، بل هي تشكل جزءاً من السجلات التجارية للمؤسسة التي تمتلك هذه البيانات. ومع أن ذلك قد يبدو صادماً، فإنه يمثل الواقع التشريعي القائم في الولايات المتحدة، وله تبعاته العميقة على حياة جميع المواطنين سواءٌ على الإنترنت أو من دونها. لذا فإن بياناتك تتسرب إلى أماكن لم تكن لترغب في وصولها إليها، ولا يمكنك استرجاعها مهما بذلت من جهد في سبيل ذلك.

من المفهوم إذاً أن ترد كلمة "فايسبوك" في ثلث ملفات الطلاق عام 201. فكل ما سبق يسهم بجدارة في لجوء 81 بالمئة من محامي الطلاق، على حد اعترافهم، إلى البحث في مواقع الوسائط الاجتماعية عن أدلة يستخدمونها ضد أزواج موكّليهم. فجميع البيانات التي تتم مشاركتها على الفايسبوك وتويتر وجميع سجلات مكالمات الهواتف الخلوية وبيانات الموقع الجغرافي التي تبين بوضوح أين ومتى كان هاتف ما بجوار هاتف آخر، تصبح لعبة عادلة في المعركة المَلَكية التي قد تكون عبارة عن قضية طلاق. فالصور التي التقطتها ببراءة في جميع تلك الحفلات على مر السنين، بنظرة تائهة وكأس في يدك، تصبح الآن دليلاً على أنك أب غير صالح وهدية من ذهب لمستشار الدفاع الخصم خلال جلسات الاستماع. والملف الذي تنشئه على موقع أوكيوبايد للتعارف وتشير فيه إلى كونك عازباً (والذي سربته بيانات متصفحك إلى خمس عشرة شركة تسويق)، سيكون مقبولاً تماماً حين تشير إليه زوجتك خلال محاكمة الطلاق. وحين يشتكي زوج من أن زوجته أم غير يقظة وغير مؤهلة، فستكون لديه أدلة جديدة قوية يدعم بها ادعاءاته، حين يستدعي سجلات توثق مئات الساعات التي كانت

تقضيها في لعب المزرعة السعيدة وعالم الأسلحة في أوقات تتقاطع مع مواعيد جميع ألعاب كرة القدم وكرة القاعدة التي فوتتها على أولادها. لكن البيانات التي نسربها تؤثر علينا لا في قضايا الطلاق وحسب، بل في فرص العمل أيضاً.

فقد بين استطلاع أجرته مايكروسوفت حول موضوع السمعة على الشبكة، أن 70 بالمئة من محترفي الموارد البشرية قد سبق لهم أن رفضوا مرشّحاً لوظيفة بناءً على معلومات كشفوا عنها خلال عملية بحث على الشبكة. والأسوأ من ذلك هو أن بعض أرباب العمل باتوا اليوم يطلبون كلمات سر الوسائط الاجتماعية من المتقدمين للعمل، بل من الموظفين الحاليين أيضاً. هل تريد العمل لدى شركة نورمان في أوكلاهوما أو في قسم الشرطة أو في قسم السلامة العامة والخدمات الإصلاحية في ميريلاند، أو في بلدية بوزمان بمونتانا أو لدى شرطة ولاية فيرجينيا؟ لقد طُلب من المتقدمين إلى جميع هذه الهيئات تسليم كلمات مرورهم على الفايسبوك أو أي من الوسائط الاجتماعية الأخرى كجزء مما يدعى "الدراسة الروتينية للخلفية"، ما يعني تمكين أرباب العمل المحتملين من الوصول إلى جميع رسائلك وصورك وتاريخ ملفك، الخصوصي والعام، على الفايسبوك وغوغل وياهو ويوتيوب وإنستغرام! وبينما منعت بعض الولايات، مثل كاليفورنيا، مثل هذه الممارسات بحق الموظفين، فإنه ما من قانون فدرالي يوقفها وتبقى قانونية في 80 بالمئة من الولايات الأميركية، ويستمر تسريب البيانات.

لا تنفك تزداد الحالات التي يطلب فيها المعلمون والمديريات التربوية هذه المعلومات من التلاميذ أيضاً، دون تفويض بالطبع. وهو ما حدث مع تلميذة إعدادية في مينيسوتا في الثانية عشرة من عمرها، حين اتهمت بنشر "تعليقات غير ملائمة" على حسابها على الفايسبوك. وكانت التلميذة في مدرسة منطقة مينيواسكا المتوسطة قد نشرت أنها "تكره" مدرّساً معيناً كان

"دائماً فظاً معها". واستدعيت الفتاة إلى مكتب المدير، حيث كان الإداريون وموجه تربوي ومعاون في انتظارها، حيث طالبوها بتسليم كلمة مرورها على الفايسبوك لكي يتمكنوا من مراجعة جميع منشوراتها. وثمة دعوى قضائية معلقة بالطبع، لكن العدد المتزايد من الحالات الاستثنائية يبين أن أبناءك يسربون بيانات قد تعود إليهم يوماً ما وتزعجهم أيضاً.

حتى الرياضيون الجامعيون في معاهد مثل جامعة كارولينا الشمالية وجامعة أوكلاهوما، بات يطلب إليهم تقديم كلمات مرورهم على مواقع الوسائط الاجتماعية إلى مدربيهم كشرط لممارسة رياضاتهم في الجامعة. بل إن بعض رياضيي الجامعات قد أجبروا على تنصيب برمجيات تنصت على حواسبهم الشخصية وهواتفهم، تقدمها شركات مثل يوديليجنس تتتبع نشاطات الطلاب بالزمن الحقيقي لضمان "تقديم أقسام الرياضة الجامعية للحماية ضد المنشورات المخربة التي تصدر عن الرياضيين الجامعيين".

أصبحت الحكومات بدورها تشارك في هذه الممارسات. فقد بين استبيان أجرته الجمعية الدولية لرؤساء الشرطة وشمل أكثر من خمسمئة مؤسسة لتطبيق القانون أن 86.1 بالمئة من أقسام الشرطة أصبحت اليوم تدرج عمليات البحث في الوسائط الاجتماعية كجزء من إجراءات التحقيقات الجنائية لديها. بل إن مصلحة الضرائب بدأت بتدريب محققيها على كيفية استخدام الشبكات الاجتماعية للتدقيق في أوضاع دافعي الضرائب رجوعاً حتى عام 2009، كما أوكلت خدمة المواطنة والهجرة التابعة للأمن الداخلي إلى عملائها عام 2010 مهمة استخدام مواقع الوسائط الاجتماعية لـ "مراقبة الحياة اليومية للمتقدّمين والمستفيدين من خدماتها ممن يشتبه بأنهم محتالون".

يمكن للعملاء الفدراليين بسهولة أن يلجوا إلى بياناتك الاجتماعية بطرق متنوعة، كمذكرات الاستدعاء ورسائل الأمن القومي وغيرها من الأوامر

الإدارية التي يمكن تقديمها إلى مزودي الخدمة الذين تتعامل معهم. ولن يكون على هؤلاء، وفقاً لقانون الطرف الثالث الذي يعفيهم من التعديل الرابع، حتى أن يُعلموك بهذه الطلبات. وقد كشفت شركة إيي.تي.إند.تي عام 2013 على سبيل المثال عن تلقيها أكثر من 300,000 طلب للكشف عن بيانات ذات صلة بقضايا مدنية وجنائية. وأتت هذه الطلبات من سلطات محلية وأخرى على مستوى الولاية وأخرى فدرالية، وكان بينها "248,000 مذكرة استدعاء، وحوالى 37,000 أمر محكمة وأكثر من 16,000 مذكرة بحث". بل إن شركة سبرينت كشفت عام 2009 أنها أنشأت بوابة مخصصة حصراً للسلطات التنفيذية، أعطت الشرطة إمكانية "لكز" أي هاتف نقال (من دون مذكرة) تشغّله الشركة بهدف تحديد أماكن المستخدمين بالزمن الحقيقي، وقد تم استخدام هذه الميزة من قبل الشرطة أكثر من ثمانية ملايين مرة في غضون عام واحد.

أما المعلومات التي لا تصل إليها الحكومة بمذكرة استدعاء، فإنها تشتريها. إذ لم تتمكن وكالة الأمن القومي وغيرها من الوكالات الحكومية من بناء شبكات التنصت وجمع البيانات العالمية من لا شيء، لكنها اشترت أو استحوذت بطرق أخرى على نسخة كاملة مما كان العالم التجاري يقوم بجمعه. والأمر منطقي تماماً، فلماذا تبني ما يمكنك ببساطة شراؤه؟ تحتفظ شركة تشويس بوينت، المملوكة اليوم لشركة ريد إلسيفير، بسبعة عشر مليار سجل لأفراد وشركات تعيد بيعها إلى 10,000 من زبائنها، بمن فيهم 7 وكالة تنفيذية محلية وفدرالية وعلى مستوى الولاية. وقد أكدت تسريبات إدوارد سنودين، أن وكالة الاستخبارات المركزية تدفع عشرة ملايين دولار لشركة إي.تي.إند.تي كل عام لقاء بيانات المكالمات، كما أشارت التسريبات إلى أن شركة فيريزون تقدم بدورها بيانات إلى حكومة الولايات المتحدة. ولم يضيع سماسرة البيانات التجاريون وقتاً لتقديم خدمات الاشتراك المدفوعة

التي يديرونها إلى عملاء الحكومات، والتي يوفرون من خلالها فيض البيانات الذي تقدمه أنت مجاناً عبر الشبكات الاجتماعية.

سخرت شبكة أخبار أونيون الكوميدية من الأحوال القائمة في تخيل عبقري قدمته على شكل تقرير إخباري مُخترع:

> أعاد الكونغرس اليوم إقرار تمويل الفايسبوك، برنامج المراقبة الشبكية الشامل الذي تديره وكالة الاستخبارات المركزية. وفقاً للتقارير، يكاد الفايسبوك يحل محل جميع برامج جمع المعلومات الأخرى التي تديرها الوكالة منذ تأسيسه عام 2004. [على لسان مسؤول مُختَلَق في وكالة الاستخبارات المركزية] "بعد سنوات من مراقبة الشعب سراً، فاجأنا استعداد كل هؤلاء الناس لنشر معلومات عن أماكنهم وعن معتقداتهم الدينية والسياسية مع قائمة مرتّبة أبجدياً بأسماء أصدقائهم وعناوين بريديهم الإلكتروني الشخصي وأرقام هواتفهم والمئات من الصور لهم، بل وحتى تحديثات حالة يصفون فيها ما يفعلونه لحظة بلحظة. إنه حقاً حلم يتحقق بالنسبة للسي.آي.إيي. ويعود الفضل في جلّه إلى عميل الوكالة مارك زوكربيرغ الذي يدير العمليات اليومية للفايسبوك لمصلحة الوكالة".

قد يبدو تقرير الأخبار المزيفة هذا مضحكاً وعفوياً، لكن معلوماتنا الشخصية التي تتسرب إلى سماسرة البيانات الذين يعملون في الظل، كما إلى الحكومات، ليست بالأمر المضحك. فتكلفة اقتصاد الرقابة، الذي يَدين بالكثير إلى التطورات الكبيرة التي شهدها إلى التقانة، تنخفض بمعدّل أسّي. ولم تعد هناك حاجة إلى فرق كبيرة من العملاء الخاصين لملاحقتك في كل مكان وتتبعك سيراً على الأقدام أو بسيارة بينما تتنقل في المدينة. فقد

قدّرت إحدى الدراسات أن استخدام برمجيات المراقبة الوكيلة التي تركز على الهواتف الجوالة والنشاطات على الإنترنت والبيانات الاجتماعية ومعلومات الموقع الجغرافي والمناقلات المالية، يكلّف الحكومة اليوم "574 دولاراً لكل دافع ضرائب، أي 6.5 سنت فقط في الساعة" لملاحقة الأميركيين فرداً فرداً.

عندما عُلم المدى الحقيقي لقدرات التجسس المحلية والدولية لوكالة الأمن القومي، اعترف فولفغانغ شميدت، الرئيس السابق لوكالة الاستخبارات الألمانية الشرقية، أو شتازي، على الملأ بأن مثل هذا النظام "كان بمثابة حلم يتحقق". ونوه شميدت إلى أنه خلال ترؤسه خدمة الشرطة السرية المرعبة في جمهورية ألمانيا الديمقراطية، لم يكن بإمكان الشتازي تسجيل أكثر من أربعين مكالمة هاتفية على مستوى البلاد في الوقت نفسه، لكن من الواضح أن التقانة باتت اليوم تسمح بمراقبة جميع الاتصالات وجميع بيانات الإنترنت طوال الوقت. وقد حذّر من أن "قمة السذاجة هي الاعتقاد بأن كل هذه المعلومات التي يتم جمعها لن يتم استخدامها... إنها طبيعة المنظمات الحكومة السرّية. والسبيل الوحيد لحماية خصوصية الناس هو منع الحكومة من جمع معلوماتهم أساساً".

المعرفة قوة، والشيفرة البرمجية هي المَلِك، وأورويل كان على حق

في روايته الديستوبية 1984، يصوّر جورج أورويل دولة رقابة حكومية شاملة تحكمها نخبة صغيرة تتمتع بامتيازات خاصة كانت تدين التفكير المستقل باعتباره "جريمة ذهنية". ومع أن أورويل كان سيتنبأ بدقة بكارثة وكالة الأمن القومي، إن.إس.إيي، فإنه ليس واضحاً أنه كان سيتنبأ بشركة أكسيوم ومواقع فايسبوك وغوغل. ففي هذه الحالات لم تكن حكومة "الأخ الأكبر" هي التي "فعلت شيئاً بحقنا"، بل نحن من فعل شيئاً بحق نفسه. فقد سمحنا بالاستفادة منا مالياً وتحويلنا إلى سلع رخيصة، متخلين عن

بيانات شخصية قيمتها تصل إلى مليارات الدولارات لمصلحة فئات جديدة من النخب التي رأت فرصة سانحة فاغتنمتها. فنحن من كان يوافق على جميع اتفاقيات الخدمة المعدة من طرف واحد دون حتى أن نقرأها، وكانوا هم يعظّمون أرباحهم دون أن تقف في وجههم أية تشريعات أو رقابة. ولا شك في أننا قد حصلنا من هذه الصفقة على منتجات رائعة، فلعبة الطيور الغاضبة ممتعة حقاً. لكن بعد أن تخلينا عن كل هذه البيانات سنجد أنفسنا تحت رحمة حيتان البيانات العظيمة التي تكاد قدراتها تضاهي قدرات الحكومات والتي باتت تفعل ما يحلو لها ببياناتنا وحيواتنا.

في كتابه المنشور عام 1999 "الشيفرة البرمجية والقوانين الأخرى في الفضاء السايبري"، يبين أستاذ كلية الحقوق في جامعة هارفرد لورنس ليسينغ بجلاء، أن التعليمات المشفّرة في أي برمجية أو تطبيق أو منصة تشكّل الإنترنت وتحدد شروطها مثلها مثل أية قوانين أو تشريعات، أي إن التغييرات التي تجريها مواقع فايسبوك وغوغل من طرف واحد على شروط خدمتها للسماح بمشاعية منشوراتك أو باستخدام صورك في الإعلانات ضد رغبتك، أشبه بـ "قوانين" جديدة تتم المصادقة عليها. فما الشيفرة البرمجية سوى قانون في الواقع.

ربما كان الطريق الوحيد للخروج من مثل هذا النظام هو أن يغلق المرء حسابه أو ألاّ ينشئ حساباً أساساً. إلا أن الحلّين، لسوء الحظ، إشكاليان ويقتربان تدريجاً من الاستحالة. وقد سبق لمقالة في نيويورك تايمز أن نوهت إلى أن الفايسبوك يحتفظ ببياناتك حتى بعد أن تغلق حسابك. فحتى حين تقرر عدم المشاركة في شبكة اجتماعية على الإنترنت، سيستمر أصدقاؤك في الإشارة إليك في الصور وسيستمر نظام الموقع الجغرافي في سيارتك بتتبّع موقعك، وستستمر متاجر تارغيت بتذكّر جميع مشترياتك.

إن الكميات غير المسبوقة من بياناتنا التي نعهد بها إلى شركات خاصة هي لقمة سائغة، وبعد أن يخرج الجني من القمقم ما من وسيلة لإعادة حبسه. فالفرصة الثلاثية الناتجة عن استنزاف بياناتنا على الإنترنت مع اتفاقية الخدمة التافهة وقلة أو غياب التشريعات تسمح لسماسرة البيانات المعاصرين بمراقبتنا، بقدرات رقابية تفوق القدرات الحكومية. فهم يلتقطون كل فكرة تخطر لنا أو صورة نظهر فيها أو موقع نمر به ويخضعونها كلها إلى تحليلات البيانات الكبيرة. وكما كان على كل من مات هونان وبلال أحمد ومايك سيي وبوبي دونكان ولاي فان بريان وإيميلي بونتينغ جميعاً أن يتعلموا بأنفسهم، فإنه ثمة تكاليف ومجازفات اجتماعية يفرضها التسرب المستمر لبياناتنا. لكن الآثار المتعلقة بالخصوصية ليست سوى واحدة من التهديدات الكبرى الناتجة عن النمو الأسّي للبيانات.

يعمل القراصنة بدأب على سرقة جميع البيانات الاجتماعية التي تقدمها طواعية عن نفسك، وكثيراً ما ينجحون في الولوج إلى حواسب سماسرة البيانات وعمالقة الإنترنت المسؤولين عن تخزين كل ذلك. وكما تعلم كل من سوني وتارغيت، بل وحتى وزارة الدفاع، فإن البيانات المخزنة في نظم المعلومات غير الآمنة ليست سوى بيانات تنتظر من يستولي عليها. لذا فإن جميع البيانات التي يتم جمعها ستتسرب في النهاية، وسيكون لذلك آثار هائلة تقع على حياتنا الشخصية والمهنية بل وحتى على سلامتنا وأمننا.

المشكلة في تحولنا إلى منتج بعد أن كنا الزبون بالنسبة لسماسرة البيانات الشاملة تكمن في أننا لم نعد نتحكم ببياناتنا، فصارت مصائرنا خارج أيدينا. فالتجميع المستمر لهذه المعلومات على نحو غير مضبوط وغير آمن، أشبه بقنبلة موقوتة مع توفر كل فكرة تخطر لنا وكل فعل نقوم به لمن يريد تلقفها من الفئات الجديدة الناشئة من الفاعلين السيئين، الذين يذهبون في نواياهم إلى ما هو أسوأ من مجرد بيعنا حفاضات بسعر مخفّض أو تحسين

رسوم تأميننا. فعصابات الجريمة المنظمة الدولية والحكومات المارقة وحتى الإرهابيون يدأبون على تكريس سمسرة بيانات خاصة بهم وعلى شحذ قدراتهم التحليلية بهدف استغلال أكبر منجم يصادفونه على الإطلاق، وسيكون لذلك آثار مرعبة تطالنا جميعاً.

الفصل السادس
بيانات كبيرة، مخاطر كبيرة

قدراتنا التقانية في ازدياد، لكن الآثار الجانبية والأخطار الكامنة تتصاعد أيضاً.

ألفين توفلر

في أمسية السادس والعشرين من شهر تشرين الثاني عام 2008، نزل رجل في التاسعة والستين في الغرفة رقم 632 في فندق تاج محل بالاس الفاخر، في مدينة مومباي الهندية. وكان النزيل، واسمه ك.ر. رامامورثي، زائراً من مدينة بانغالور في رحلة عمل روتينية، ولم يكن يدري على الإطلاق بأن حياته كانت على وشك أن تتغير مرةً وإلى الأبد.

فعند الحادية عشرة مساءً تقريباً، سمع رامامورثي جلبة قصيرة خارج غرفته، ليقرع الباب بعدها فجأةً: "خدمة الغرف". كان رامامورثي يعلم أنه لم يطلب أي طعام، فشعر بأن شيئاً ما خطيراً يجري. لكنه حين حاول التراجع نحو الحمام، ارتطم من دون قصد بالباب، فوشى صوت الارتطام بوجوده داخل الغرفة، وكان الرد على ذلك سريعاً، إذ اخترق وابل من الرصاص الباب مزيلاً القفل الذي يفصل رجل الأعمال عن العالم الخارجي.

اقتحم رجلان مدججان بالسلاح غرفة رامامورثي، الذي ضُرب وخلعت ملابسه وتم تقييده بلمح البصر في ليلة أصبحت بالنسبة إليه أرهب ليلة في حياته. كان الرجلان تابعين لمنظمة إرهابية باكستانية تابعة لتنظيم القاعدة، تعرف باسم لاشكار - إي - طيبة. لقد وجد تعيس الحظ رامامورثي نفسه في وسط الحصار الإرهابي القاتل لمدينة مومباي عام 2008.

"من أنت، وماذا تفعل هنا؟" سأله آسروه من جماعة لاشكار. "أنا مجرد أستاذ مدرسة بريء"، أجابهم رامامورثي. وكان الإرهابيون بالطبع يعلمون أنه لا يمكن لأستاذ مدرسة هندي المكوث في جناح أحد أكثر الفنادق

رفاهية. ثم كان أن وجد الإرهابيون بطاقة هوية رهينتهم على دولاب السرير، ليصبح لديهم الآن اسمه الحقيقي الذي أعطوه إلى قادتهم الإرهابيين بواسطة هاتف يعمل بالأقمار الصناعية كان بحوزتهم.

تلقى مركز عمليات المنظمة المكالمة كما يحدث في أي مركز تحكم وقيادة عسكري حديث. فانطلاقاً من الحدود الباكستانية، كان قادة المنظمة الإرهابية يتابعون سير هجومهم على المواطنين في مومباي. فقاموا باختيار أهدافهم بدقة، وكان من بينها فندقان فاخران ومحطة قطار مكتظة ومركز اجتماعي يهودي ومقهى شعبي للسياح، بل مستشفى للنساء والأطفال. وعلى أرض مدينة مومباي، قام منفذو العمليات الإرهابية بوحشية بإلقاء قنبلتين يدويتين على الناس الذين كانوا يأكلون في المطاعم، كما أطلقوا النار على مدنيين عزل كانوا ينتظرون القطارات للعودة إلى منازلهم بعد فراغهم من عملهم.

بعد أن انتشرت أخبار الهجمات، قبع قادة المنظمة في باكستان في غرفة الحرب لديهم يراقبون شبكات بي.بي.سي والجزيرة وسي.إن.إن والتلفزيون المحلي الهندي، ليعرفوا قدر المستطاع كيف تسير العمليات وما هو رد فعل الحكومة الهندية. ولم يكتف الإرهابيون في جمع معلوماتهم على وسائل البث فقط، بل كانوا أيضاً ينقّبون في الإنترنت ومواقع التواصل الاجتماعي بالزمن الحقيقي ليحققوا أثراً مميتاً.

فعندما قبض الإرهابيون على راماورثي، أجروا اتصالاً باسمه مع قاعدتهم في باكستان، حيث قام مركز العمليات بإجراء بحث بارع عن رهينتهم على الإنترنت. وما كانت إلا لحظات حتى وصلوا إلى صورته ثم إلى مكان عمله. فعلموا أن راماورثي لم يكن أستاذاً بريئاً كما ادعى عندما ناشدهم إبقاءه على قيد الحياة، بل إنه في الحقيقة رئيس أحد أضخم مصارف الهند، مصرف "إنغ فيزيا". واستناداً إلى الصورة التي وجودها على الإنترنت، طلب القادة

الإرهابيون من منفذي العملية في فندق تاج محل بالاس أن يقارنوا بين الرجل الذي معهم وبين صورة رئيس البنك الموجودة على الإنترنت:

- هل الرهينة قصير وبدين؟
- نعم.
- هل هو أصلع الجبهة؟
- نعم.
- هل يضع نظارات؟
- نعم.

"ماذا نفعل به؟" سأل مُعتقلو رامامورثي. وبعد لحظات أتاهم جواب غرفة العمليات. اقتلوه.

في لحظة، كان مجرد بحث بسيط على الإنترنت هو كل ما يحتاج إليه الإرهابيون ليقرروا مصير الرجل الكهل. إذا كان سوء استخدام إعدادات الخصوصية على الفايسبوك من قبل المعلنين وسماسرة البيانات مصدر قلق لنا، فإن الواقع هو أن انفتاحنا يمكن أن يُستخدم ضدنا بطرق أسوأ من أي شيء يمكننا تصوره. فالبيانات التي نسربها لا تحصل عليها الشركات والحكومات وحدها. فالمجرمون والإرهابيون أيضاً يدخلون إلى بياناتنا الاجتماعية ويبسطون سيطرتهم عليها بدقةٍ قاتلة. في عالم اليوم، يمكن لمحرك البحث أن يحدد بمعنى الكلمة من يجب أن يعيش ومن يجب أن يموت.

كانت بحوزة الرجال الذين نفذوا الهجوم على مومباي بنادق من نوع إيي.كي - 47 ومتفجرات آر.دي.إكس. وإذا كانت البنادق والقنابل ليست بالشيء الجديد في العمليات الإرهابية، فإن هؤلاء المنفذين كانوا يمثلون نوعاً جديداً ومقلقاً من الإرهابيين. فقد استشفّوا المستقبل وكانوا يستغلون تقانات المعلومات الحديثة في كل خطوة كانوا يقومون بها لتنفيذ هجومهم

من أجل تحديد موقع المزيد من الضحايا وقتلهم.

عندما انطلق المهاجمون نحو البحر من باكستان تحت جنح الظلام، كانوا يضعون نظارات للرؤية الليلية ويمخرون البحر نحو مومباي، بمساعدة أجهزة تحديد مواقع (جي.بي.إس). وكانت في حوزتهم أيضاً هواتف بلاك بيري توجد فيها ملفات بي.دي.إف تحتوي على خرائط لسطح الفندق، كما استخدموا موقع غوغل إيرث لاستكشاف النماذج الثلاثية الأبعاد للمواقع المستهدفة، لتحديد أفضل نقاط الدخول والخروج. وأثناء الهجوم، استخدم القتلة هواتف تعمل على الأقمار الصناعية وأجهزة نقالة دولية وبرنامج سكايب في التنسيق مع مركز قيادتهم في الباكستان، الذي كان بدوره يراقب إذاعات الأخبار والإنترنت ومواقع التواصل الاجتماعي لكي يوفر تعليمات تكتيكية لفريقه العامل على الأرض بالزمن الحقيقي.

عندما التقط المارون صورة لفرقة المغاوير التابعة للشرطة وهي تنزل من الطائرة على سطح المجمع اليهودي المحاصر، تلقف مركز العمليات الإرهابي الصورة ليحذر المهاجمين ويوجههم نحو بيت الدرج الذي يقود نحو السطح. ما إن فتحت قوات الشرطة، التي كانت تأمل مفاجأة الإرهابيين، الباب حتى وجدت نفسها في كمين داخل بيت الدرج. وعندما ذكرت محطة بي.بي.سي على الهواء مباشرة أن شهوداً عياناً ذكروا أن الإرهابيين كانوا يختبئون في الغرفة 360 أو 361، اتصلت غرفة العمليات بهم مباشرة وأخبرتهم بضرورة تغيير موقعهم لكي لا يقعوا بيد الشرطة.

في كل مرحلة من مراحل الحصار، كان المهاجمون يستغلون التكنولوجيا المتوفرة لديهم بسرعة لكي يدركوا موقعهم وليحافظوا على تفوقهم التكتيكي على قوات الشرطة والحكومة. فقاموا بمراقبة الإنترنت ووسائل التواصل الاجتماعي وجمعوا كافة البيانات المتاحة، بل قادوا عملية استخبارات مضادة محكمة على الإنترنت لحماية المنفذين. كان الإرهابيون خلال هجوم

مومباي في غاية الاعتماد على التقانة، حتى إن الكثير من الشهود أشاروا إلى أنهم رأوا المنفذين يطلقون النار على الرهائن من بنادقهم باليد اليمنى بينما يحملون هواتف بلاك بيري بيدهم اليسرى في الوقت نفسه ليعاينوا الرسائل القادمة إليهم من المركز.

لم تكن التقانة عاملاً حاسماً في نجاح عملية الحصار وحسب، بل إن استغلالها الإجرامي، كما رأينا في الفصل الأول، موّل الهجوم. فقد كانت خلية قرصنة فيليبينية تعمل إلى جانب الجماعة الإسلامية التابعة للقاعدة قد نفذت جريمة إلكترونية واسعة وعملية احتيال على الإنترنت لتمويل العملية في الهند. إذ قام القراصنة بإعادة تحويل الملايين من المكاسب الإلكترونية غير الشرعية إلى مدربيهم، ليقوم هؤلاء بدورهم بغسيل هذه الأموال وإرسالها لجماعة لاشكار - إي - طيبة المسؤولة عن الهجوم على المدنيين في مومباي.

وفي النهاية، استغرقت الشرطة ثماني وستين ساعة لإنهاء الحصار في مدينة مومباي. وتمكنت الفرق المضادة للهجوم في النهاية من قتل تسعة من الإرهابيين وإلقاء القبض على العاشر. وكان من المفاجئ أن أحد الأبرياء الناجين من الهجوم كان ك.ر.رامامورثي. ففي اللحظة التي أصدر فيها مركز قيادة لاشكار - إي - طيبة الأمر بقتله، حدث انفجار في فندق تاج محل بالاس فظن المهاجمون أن الشرطة تقترب منهم. ومنح هرع الإرهابيين للتحقق من الأمر راماموري لحظة قصيرة كانت كافية ليحرر نفسه ويهرب. لكن حظ 166 رجلاً وامرأة وطفلاً آخرين كان مختلفاً، فقد قضوا في ذلك اليوم، إضافة إلى مئات الأشخاص الذين تعرضوا لجراحٍ بالغة نتيجة تلك المجزرة.

لنتوقف للحظة ونفكر بمعاني هذا الهجوم الإرهابي. عشرة رجال مسلحين، ليس فقط بالأسلحة بل بالتقانة، كانوا قادرين على شل حركة مدينة فيها

حوالى اثنا عشر مليون نسمة وتعدّ رابعة أكبر مدينة في العالم، في حدثٍ تمت تغطيته مباشرةً حول العالم. وقد أثبت المهاجمون أنهم قادرون تماماً على جمع وتبادل المعلومات الاستخبارية المتاحة (وسائل الإعلام التقليدية والإنترنت والهواتف النقالة والبيانات الاجتماعية) لتنفيذ هجوم اعتراضي واستخدام هذه المعلومات في اتخاذ قرارات عملياتية متزامنة. كانت جماعة لاشكار - إي - طيبة ببساطة تعالج البيانات التي يسربها عامة الناس لتستغلها بالزمن الحقيقي لتقتل المزيد من الناس وتضمن تفوقها على السلطات. هكذا كان الإرهاب في العصر الرقمي في عام 2008. فما الذي يمكن للإرهابيين فعله بالتقنيات الموجودة اليوم؟ وما الذي سيفعلونه بتقنيات المستقبل؟ إن الدرس الذي تعلمنا إياه تجربة مومباي هو أن التغير الأسّي لا ينطبق على الأخيار فقط، بل على الأشرار أيضاً.

البيانات هي النفط الجديد

كل شيء حولنا يواظب على إنتاج البيانات. كل إجرائية رقمية أو جهاز استقبال أو هاتف نقال أو جهاز موقع جغرافي، أو محرك سيارة أو فحص مخبري طبي أو معاملة ببطاقة ائتمانية أو قفل غرفة في فندق أو تقرير مدرسي، أو تبادل يجري على مواقع التواصل الاجتماعي، كلها تقوم بتوليد البيانات. تحول أجهزة الهاتف الذكية البشر إلى أجهزة حساسات بشرية تولد كميات هائلة من المعلومات. لذا فإن الأطفال الذين يولدون اليوم سيمضون حياتهم كلها مع هذا الأثر الرقمي الواسع، مع توفر حيز على الإنترنت يقدم عبره حوالى 92 بالمئة من الأطفال أنفسهم. فاعتباراً من المنشورات الأولى التي يضعها آباؤهم عنهم لنشر صورهم وهم في الرحم، وحتى فصل المنبه القلبي الموصول بالإنترنت بعد ذلك بمئة عام، سوف تسجل كل لحظة من الولادة وحتى الموت رقمياً ليتم الاحتفاظ بها في السحابة الرقمية إلى الأبد. ودورة خلق البيانات لدينا لا تتوقف أبداً، ففي

عام 2014 كنا في كل دقيقة من كل يوم:

- نرسل 20,166,667 بريداً إلكترونياً.
- نبحث في محرك البحث غوغل مليوني مرة.
- نشارك 684,000 موضوع على الفايسبوك.
- ننشر 100,000 تغريدة على تويتر.
- نحمّل 47,000 تطبيق من متجر تطبيقات أبل.
- نحمّل مواد فيديو مدتها 48 ساعة على اليوتيوب.
- نضع 36,000 صورة جديدة على إنستاغرام.
- نكتب 34 مليون رسالة على واتس أب.

بعبارة أخرى، كنّا في كل عشر دقائق نخلق كمية من المعلومات تعادل تلك التي نشأت عن العشرة آلاف جيل الأولى من البشر. كذلك الأمر، فإن تكلفة تخزين هذه البيانات تنخفض نسبياً. ففي أواخر عام 2014 على سبيل المثال، كان يمكن شراء سواقة تخزين بسعة 6 تيرابايت من موقع أمازون مقابل 300 دولار فقط لتخزين جميع الموسيقى التي سبق أن سُجلت في أي مكان في العالم وعبر التاريخ.

لُقّب هذا النموّ الواسع في البنية التحتية المعلوماتية في العالم بلقب ثورة البيانات الكبيرة، التي تَعِد بجعل المشاكل المعقدة العالقة قابلة للرقمنة لتصبح قابلة للحل تجريبياً. ففي مجال الطب، بعد أن تم تصنيف جميع بيانات المرضى على سجلات طبية إلكترونية، أصبح من الأسهل على الأطباء التنقيب في مجموعات البيانات هذه لتحديد العلاج الأنجع واكتشاف التفاعلات البينية القاتلة للأدوية، بل وحتى التنبؤ ببداية المرض قبل ظهور أعراضه الجسدية. أي إنه من الممكن إنقاذ أرواح لا تُعد ولا تُحصى.

عبر كافة الصناعات، سواء البيع بالتجزئة أو النقل أو الأدوية، ستنتج قيمة اقتصادية هائلة عن هذه البيانات الكبيرة، حتى إن المنتدى الاقتصادي العالمي قد أطلق مؤخراً على البيانات اسم "الوقود الجديد". فثمة حمى ذهب جديدة تتمثل في إعادة التنظيم المستشرية من قبل شركات عديدة، مثل آي.بي.إم وأوراكل وساس ومايكروسوفت وساب وإي.إم.سي وإتش.بي وديلّ لأعظمة الأرباح التي تعود عليها من ظاهرة البيانات الكبيرة. وإذا كانت البيانات تمثل الوقود الجديد والعملة الحديثة للعالم الرقمي، فإن أولئك الذين يمتلكون الكميات الكبرى منها سيكون لهم سطوة ونفوذ هائلان. فتماماً كما كان سادة البترول الأوائل، من أمثال جون د.روكفيلر وج.بول غيتي، يستأثرون بالسلطة في زمنهم، كذلك سيكون أولئك الذين يملكون أكبر مقدار من البيانات في العالم الحديث، كما يتبين من مارك زوكيربيرغ وإريك شميدت. تقوم شركات مثل فايسبوك وغوغل وأكسيوم بإنشاء أضخم مجموعة من البيانات عن السلوك البشري يتم جمعها في تاريخ البشرية، وبإمكان هذه الشركات استغلال هذه البيانات لأغراضها الخاصة، مهما كانت هذه الأهداف، سواء كانت الربح أو المراقبة أو البحث الطبي أو القمع السياسي أو الابتزاز.

لكن إذا كانت البيانات هي النفط الجديد، فلا بد من حراستها أسوة ببقية المصادر الطبيعية المعروفة. فنحن لا ندع 100 مليون برميل من النفط دون حماية، لكن هذا بالضبط هو ما يفعله معظمنا بأغلبية البيانات التي نخلقها. فدرجة حمايتنا للمعلومات الرقمية أبعد ما تكون عن المستوى المطلوب. والمئة مليون برميل من النفط التي ذكرناها تتم حمايتها بالحراس والأسوار والأسلحة وكاميرات المراقبة وأجهزة الاستقبال على الأرض على طول خطوط الأنابيب النفطية، لكن ماذا عن المئة مليون بطاقة ائتمان وسجلات الزبائن المخزنة لدى باعة مثل متاجر تارغيت؟

تخزن تلك البيانات، كما رأينا سابقاً، في قواعد بيانات غير آمنة وضعيفة الحماية بطبيعتها.

عندما تقوم بجمع هذا الكم الهائل من البيانات القيمة وتفشل في حمايتها، ماذا سيحدث برأيك؟ إن قدرتنا على كسب وتخزين المعلومات تفوق بكثير قدرتنا على فهمها وفهم آثارها. فبالرغم من أن التكاليف العملية لتخزين معلومات العالم تقترب من الصفر، فإن التكاليف الاجتماعية لها قد تكون أعلى بكثير، ما يخلق مسؤوليات مستقبلية هائلة تقع على عاتق المجتمع والعالم.

يمكن للتاريخ هنا أن يؤدي دوراً توجيهياً. فقد كان ويلي سوتون، لص البنوك الأميركي المشهور، قد سرق مليوني دولار تقريباً على مدى عقود من سيرته الإجرامية التي بدأت في عشرينيات القرن الماضي. وبعد أن ألقي القبض عليه على يد مكتب التحقيقات الفدرالي، سأله أحد الصحافيين: "ويلي، لماذا تقوم بسرقة البنوك؟"، فكان جوابه الذي كثيراً ما كرره "لأنها المكان الذي يوجد فيه المال". فمع أنه كان بإمكان سوتون أن يسرق مليوني شخص بمعدل دولار واحد من كل منهم، فإنه اختار أسلوباً منطقياً وموفراً للوقت حين قرر سرقة مكان تجميع العملة، أي البنوك. فهل من عجب في أن يلاحق المجرمون شركاتٍ مثل تارغيت وسوني وغيرها من الشركات الجامعة للبيانات حيث تكون الفوائد عالية والمخاطر قليلة؟ في عالمنا الحالي، أينما تكن البيانات تكن الأموال.

مستلهماً غوردون مور والقانون الذي يحمل اسمه، وضعت بدوري قاعدة أصف من خلالها المخاطر المرتبطة بالجبال المتزايدة من البيانات التي يتم خلقها. وها أنا أقدم لكم قانون غودمان:

بقدر ما تنتج وتخزن من البيانات، تكون الجريمة المنظمة سعيدة باستهلاكها.

ففي النهاية، ستقع التفاصيل الشخصية عن حياتك بيد الجماعات الإجرامية والمتنافسين، بل وحتى الحكومات الأجنبية. وإذا كانت البيانات هي النفط الجديد، فإن بياناتنا الشخصية تشبه إلى حد كبير البلوتونيوم المعد لأهداف التسلح، خطير وطويل الأمد، وما إن يتسرب حتى تستحيل استعادته ثانية.

حتى الحكومة الفدرالية تعي أنها قد تكون ضحية لهذه المشكلة. ويكفي أن نلقي نظرة على مفاجأة ويكيليكس عام 2010 ومئات آلاف البرقيات الدبلوماسية السرية، التي استطاع الرقيب تشيلسيا (برادلي) مانينغ سرقتها أثناء عمله في الجيش كمحلل استخباري في العراق. ولم تمض بالطبع سوى سنوات قليلة ليتعرف العالم إلى إدوارد سنودين الذي استخدم مهاراته وصلاحياته كمدير نظام في وكالة الأمن القومي، ليسرق ملايين الملفات عالية السرية من أميركا وحلفائها ويشاركها مع الصحافيين والعامة على الإنترنت. وقد أطلق البعض على هذا النوع من السرقة الضخمة للمعلومات وفضحِها اسم "العصيان المدني لعصر المعلومات". لكن إذا كان مانينغ وسنودين قد تمكنا (بعد تحقيقات خلفية واسعة كما هو مزعوم) من تجميع وسرقة هذه الكميات الهائلة من البيانات الحساسة من الحكومة الفدرالية، فماذا كانا ليفعلا لو كانا يعملان لمصلحة تارغيت أو سيتي بانك أو أبل؟ هذا النمو الأسّي في كميات البيانات التجارية، يعني أن الأسرار التجارية والتصاميم الهندسية والخبرة التقنية وقوائم الزبائن وجداول رواتب الموظفين واستراتيجيات تقييم الأسعار والمزودين وأية معلومات أخرى مخزنة على أي جهاز رقمي، يمكن أن تُسرّب. ففي أية شركة، كبيرة أو صغيرة، يمكن اليوم أن يكون ثمة سنودين وأن يكون له أثره الملحوظ على أمننا وخصوصيتنا وقابلية حياتنا الاقتصادية على المدى الطويل.

من خلال اختراق البريد الإلكتروني لحسابٍ واحد لدى فايسبوك أو غوغل

أو أبل، يمكن للقراصنة الولوج إلى سنوات من رسائل البريد الإلكتروني والمواعيد والرسائل السريعة والصور والمكالمات الهاتفية وتواريخ عمليات الشراء على أمازون والحسابات المصرفية، وحسابات العمولة والوثائق المخزنة على دروب بوكس أو غوغل درايف. ومن المهم أن ننوه على أية حال إلى أن خسائر البيانات التي نتصورها اليوم ستبدو تافهة إذا ما قورنت بما سيتوفر منها في المستقبل. ففي هذا العالم، تتفوق قدرتنا على تجميع كافة المعلومات الصادرة عن الإنسان أو الآلة وتخزينها إلى لأبد تفوقاً هائلاً على فهمنا للمخاطر المرافقة لها.

مضيفون سيئون أم ضحايا جيدون، أم كلاهما؟

ما كنت أفعله في شبابي بات أسهل بمئات المرات اليوم
فالتكنولوجيا تولّد الجريمة
فرانك دبليو. أباغنيل

عندما تعرضت شركات سوني وتارغيت وتي.جي.ماكس للقرصنة، من كان المخطئ؟ هل كانت هذه الشركات بريئة وقعت ضحية هجمات إلكترونية بارعة ومبتكرة نفذتها عصابات إجرامية منظمة ومتطورة عابرة للحدود؟ أم أنها كانت متراخية في إجراءات الحيطة الأمنية لديها ومقصرة في تطبيق قواعد الحماية لمئات ملايين الحسابات التي كانت مؤتمنة عليها؟ الجواب يكمن في مكان ما بين النقيضين. فالأمر لا يقتصر على عدم فعالية جهود متاجر التجزئة في حماية بيانات زبائنها، بل ثمة أيضاً أعداد كبيرة من شركات الإنترنت الناشئة وعمالقة التواصل الاجتماعي التي تعاني المشكلة ذاتها. فعندما تتبرع ببياناتك للفايسبوك وغوغل ولينكدإن وغيرها من مواقع التواصل الاجتماعي، يجب أن تكون حذراً لا فقط من العواقب الكثيرة المتعلقة بالخصوصية الناجمة عن ذلك، بل من التبعات الإجرامية أيضاً، إذ تتعرض هذه الشركات للقرصنة بشكلٍ روتيني، والبيانات المسروقة

هي ملكك. كم يتكرر هذا عادةً؟ بوتيرة لا يمكنك تصورها إطلاقاً.

اعترف قسم الأمن التابع لدى فايسبوك فجأةً بأن أكثر من 600,000 حساب يتعرض للاختراق كل يوم. هل استوعبت ذلك؟ 600,000 حساب في اليوم الواحد لا في السنة أو في الشهر. هذا يعني حساباً واحداً كل 140 جزءاً من الثانية (تستغرق طرفة العين 300 جزء من الثانية). وكلها بيانات يمكن استخدامها لسرقة الهوية والانتحال لأغراض إجرامية والتهرب من الضرائب وفي عمليات الاحتيال المرتبطة بالضمان الصحي وغيرها من الاعتداءات الإجرامية. فانظر إلى الكميات الهائلة من البيانات الشخصية التي تشاركها على الفايسبوك، وفكر فيما يمكن أن يفعله المجرمون المنظمون بها. اسم عائلة الأم، ومكان الولادة، وتاريخ الميلاد، وصور أطفالك، كلها ستصبح في قبضتهم.

ليس اختراق حسابك على الفايسبوك هو الهدف النهائي، بل ما هو سوى البداية. فبما أن 75 بالمئة من الناس يستخدمون كلمة السر نفسها في مواقع عديدة و30 بالمئة يستخدمون معلومات الدخول نفسها في كافة نشاطاتهم الإلكترونية، حالما يتم اختراق كلمة سر حسابك على الفايسبوك يمكن استخدامها للدخول إلى حسابك المصرفي أو بطاقتك الائتمانية أو حسابات بريدك الإلكتروني. إضافة إلى ذلك، تسمح لك الشركات الأخرى مع الوقت باستخدام بيانات دخولك على الفايسبوك كجواز سفر إلى بقية أرجاء العالم الرقمي. فعندما تستخدم حسابك على الفايسبوك للتسوّق أو الاستماع إلى الموسيقى أو ممارسة الألعاب، وهو أمر مريح ومناسب، سيكون لاختراق كلمة سرك على الموقع تبعاته على كافة تلك الخدمات.

سبق أن تعرضت شركات تواصل اجتماعي كثيرة للاختراق، وكان من بينها شركة لينكدإن (6.5 ملايين حساب) وشركة سنابشات (4.6 ملايين اسم حساب ورقم هاتف)، وغوغل وتويتر وياهو! والعصابات الإجرامية المنظمة

العابرة للحدود مسؤولة عن تنفيذ 85 بالمئة من هذه الاختراقات بهدف إعادة انتقاء أكبر قدر ممكن من البيانات لتحقيق أعلى قيمة في الأوساط السايبرية السرية. بل إن الجماعات الإجرامية أحياناً لا تحتاج لاختراق نظام الحاسب، فهو أصلاً مشرع الأبواب. وتماماً كما الوحوش المفترسة التي تجوب سهوب سيرينغيتي فلا تدع حيواناً ميتاً يفوتها بل تنقض عليه كوجبة مجانية، كذلك القراصنة يسعدون باستغلال أية بيانات مجانية تظهر في طريقهم. وهو ما حدث، على سبيل المثال، عندما قامت الشركة الضخمة للتخزين السحابي للبيانات دروب بوكس خطأً بإلغاء الحاجة إلى أية كلمة سر لأي حساب كان عبر شبكتها عام 2011، فكانت النتيجة أن أي شخص كان يستطيع قراءة أي ملف موجود على شبكة دروب بوكس.

قد يخطر ببالك أنه في حال تم اختراق حسابك على الإنترنت في مواقع التواصل الاجتماعي بهذه الطريقة ووقع عليك ضرر، كأن تقع ضحية انتحال هوية أو تفقد عشرات الآلاف من الدولارات من حسابك المصرفي، ناتج عن إهمال أحدهم، فإن ذلك يخولك بمقاضاة أولئك الذين عرّضوا معلوماتك للخطر، لكن الأمر ليس كذلك بالطبع. فقد تنازلتَ عن جميع تلك الحقوق عندما أكدت أنك "قرأت ووافقت على معايير وشروط الخدمة"، وهو توضيح يبرّئ تلك الشركات تماماً من الأذى الناجم عن مثل هذه الاختراقات.

والفايسبوك واضح في هذا الصدد:

> نحاول الحفاظ على الفايسبوك قيد العمل وخالياً من الثغرات وآمناً، ولكنك تستخدمه على مسؤوليتك الخاصة. فنحن نقدم لك الفايسبوك هكذا كما هو دون ضمانات صريحة أو ضمنية... نحن لا نضمن بقاء الفايسبوك آمناً ومنيعاً وخالياً من الأخطاء على الدوام... أنت تعفينا نحن

ومديرينا وموظفينا وعملاءنا من أي ادعاءات وأضرار، معروفة أو غير معروفة، ناجمة عن أو على صلة بأي ادعاءٍ صادرٍ عنك.

ليست عصابات الجريمة المنظمة، بالمناسبة، وحدها من يسعى وراء مخازن البيانات الهائلة التي قمت بإنشائها على غوغل وياهو! وفايسبوك؛ بل الحكومات الأجنبية والمحلية أيضاً. ففي كانون الثاني من عام 2010 على سبيل المثال، خرج غوغل على الملأ بأخبار عن تعرض شبكته لهجوم واسع، محمّلاً الحكومة الصينية المسؤولية عن الهجوم. وأشار غوغل في تقريره إلى أن السلطات الصينية كانت تلاحق حسابات جيميل الخاصة بناشطين في الولايات المتحدة وآسيا وأوروبا، كانوا يعبّرون عن قلقهم حيال الممارسات الصينية في مجال حقوق الإنسان، كما استُهدف في هذه الحادثة كل ما لدى غوغل من أسرار تجارية وشيفرة مصدرية، أي البرنامج المشغل لغوغل وجميع منتجاته.

مع أن غوغل اعترف بتعرضه للهجوم، إلا أن حجم وطبيعة ما تم الاستحواذ عليه بات سراً مكتوماً من أسرار الشركة. لكن سرعان ما تبين أن القراصنة المرتبطين بجيش التحرير الشعبي الصيني قد أخذوا الشيفرة المصدرية لنظام غوغل العمومي لإدارة كلمات السر. ومن الواضح أن سرقة الشيفرة المصدرية لغوغل أمّنت للصينيين وصولاً مستمراً إلى كلمات مرور الملايين من زبائن غوغل في أنحاء العالم، كما أنها سمحت لجيش التحرير الشعبي الصيني بأن يبقى متخفياً داخل أنظمة غوغل على المدى الطويل. هل غيرت كلمة مرورك على غوغل بعد عام 2010؟ إذا لم تكن قد غيرتها فإن جيش التحرير الشعبي الصيني ربما لديه نسخة عنها. وسواءٌ كانت شركات الإنترنت والبيانات الاجتماعية تسيء إدارة بياناتنا أم كانت ضحية مستهدفة إلى حد كبير، أو أنها تجمع بعضاً من الاثنين، حقيقة الأمر هي أن

أية بيانات نضعها في عهدة المواقع الإلكترونية أو الشركات يمكن أن تُسرّب إلى المجرمين والإرهابيين وغيرهم.

سماسرة البيانات بدورهم أمناء سيئون على بياناتك

إحدى المشكلات الناجمة عن وجود سماسرة بيانات غير مضبوطين يجمعون عنّا كميات هائلة من المعلومات، تكمن في أن هذه الشركات يمكن أن تتعرض بسهولة للقرصنة. فعندما تخزن شركات مثل أكسيوم تريليونات السجلات التي تحتوي معلومات عن كل واحد منّا، فإن هذه السجلات ستتعرض للاستهداف من قبل الجريمة المنظمة لأنه، وكما يُذكّرنا ويلي سوتون، هناك تكمن الأموال. وهذه السرقة الواسعة النطاق للبيانات من سماسرة البيانات جارية على قدم وساق منذ سنوات عديدة، فبين عامي 200 و2003 تمت سرقة أكثر من 1.6 مليار سجل من شركة أكسيوم وعملائها. والوثائق القضائية تبين أن القرصان المسؤول عن السرقة، واسمه سكوت ليفين، كان قادراً على تحميل أكثر من 8 غيغابايت من ملفات أكسيوم، ما يجعل هذه الحادثة من بين أكبر حالات التسلل المتضمنة لسرقة بياناتٍ شخصية على الإطلاق.

في ما بعد، في عام 2013، قامت شركة إكسبيريان لسمسرة البيانات خطأً ببيع بيانات شخصية تعود لثلثي الأميركيين تقريباً إلى عصابة جريمة منظمة في فييتنام في عملية احتيال أسطورية أدت إلى جعل أرقام الضمان الاجتماعي العائدة لـ 200 مليون أميركي متاحة للصوص في أنحاء العالم. كان اسم هذه المجموعة من البيانات التي تم استحواذها "فولز"، أي الكاملة، في الأوساط السرية الإجرامية، وذلك لأنها تحتوي كافة المعلومات اللازمة للمجرمين لكي يتمكنوا من استصدار بطاقات ائتمان وأخذ قروض بأسماء ضحاياهم. وقد حدث هذا الاختراق الأمني الكبير، لأن إكسبيريان أخفقت في إجراء تحقيق احتياطي حول منظمة القرصنة الفييتنامية التي

كانت قد أسست شركة واجهة تدّعي العمل في مجال التحقيقات الخاصة في الولايات المتحدة لكي تشتري البيانات الضرورية لتنفيذ الجريمة. هل استوعبت ذلك؟ باعت إكسبيريان 200 مليون ملف لبيانات المستخدمين إلى عصابة سرقة الهويات. وفي النهاية عُرضت البيانات للبيع على العديد من مواقع القراصنة مثل موقع SuperSet.info وموقع FindGet.me، لتباع مقابل ستة عشر إلى خمسة وعشرين سنتاً فقط للسجل الواحد، ولا يُقبل الدفع إلا عن طريق مواقع التداولات غير الخاضعة للمراقبة على الإنترنت مثل موقع Liberty Reserve وWebMoney. لم تكتشف إكسبيريان هذا الاختراق وتورطها بالمسألة سوى بعد أن اتصلت بها الخدمة السرية التي كشفت المعلومات المقدمة للبيع على مواقع القرصنة.

فما السبب الذي يجعل شركة ذات سمعة جيدة تبيع علناً البيانات دون إجراء تحقيق احتياطي؟ يكمن الجواب، كالعادة، في المال. فسماسرة البيانات يجنون المال عندما يبيعون البيانات لا عندما يحمونها. وقد تبين في سياق التحقيق أن مجموعة البيانات الفييتنامية قد قُرِأت 3.1 مليون مرة على الأقل من قبل مجرمين إلى أن تمت إزالتها، ولكن بعد أن وقع الضرر بالطبع.

نظراً لسهولة توفير بيانات عن كل شخص منّا، بدأت عصابات الجريمة المنظمة اليوم بممارسة سمسرة البيانات بنفسها وباتت تؤسس شركات واجهة تؤمن معلومات مكتسبة بشكل غير مشروع عن أي هدف تحتاج إليه. وكان مثالاً على ذلك القراصنة الروس الذين أسسوا موقع Exp ليستعرضوا مروءتهم في القرصنة للجمهور المستعد للشراء، والمكون من زملاء الجريمة بكل حسن نية. بتفاخرهم بقدرتهم على الحصول على بيانات أي شخص، يقدم القراصنة خدمة تخزين مجانية لملفات الأرصدة لعدد كبير من الشخصيات العامة في مجالات السياسة وإنفاذ القانون والترفيه.

فلكي يحصلوا على بضائعهم غير الشرعية، قام اللصوص بتخريب أنظمة الحماية على موقع AnnualCreditReport.com التابع لإيكويفاكس، وتمكنوا من الحصول على كافة تقارير الأرصدة للأشخاص المستهدفين. وكان من بين من وقع فريسة لهذا الهجوم مجموعة من المشاهير مثل آشتون كوتشير وكيم كارداشيان وجي.زد وبيل غيتس وبيونسي وروبرت دي نيرو وليدي غاغا وسين كومبس. كما تم اختراق تقارير الأرصدة لعدد من الشخصيات الحكومية المرموقة مثل السيدة الأولى ميشيل أوباما ونائب الرئيس جو بايدين والرئيس السابق جورج بوش ومدير مكتب التحقيقات الفدرالي روبرت مولر، ومدير وكالة الاستخبارات المركزية جون برينان والنائب العام إريك هولدير بالإضافة إلى رئيس قسم شرطة لوس أنجلوس تشارلي بيك.

ما إن حصل فريق القراصنة في موقع Exposed.su على التقارير الائتمانية الكاملة للأشخاص المذكورين آنفاً، حتى وضعوها على الإنترنت ضمن ملف بي.دي.إف. فبات بإمكان العالم أجمع أن يتصفح أرقام الضمان الاجتماعي للضحايا وتاريخ ميلادهم وكل عنوان قاموا باستخدامه على الإطلاق وأرقام هواتفهم الشخصية والأحكام القضائية التي وقعت عليهم وغيرها من المعلومات الشخصية الهامة، كمئات آلاف الدولارات التي يقيدونها كل شهر على بطاقات ائتمان أميريكان إكسبريس أو ملايين الدولارات التي يدينون بها لرهاناتهم العقارية. وتمت مشاهدة التقارير الائتمانية الخاصة للمتضررين مليون مرة تقريباً قبل إسقاط المواقع الإلكترونية في النهاية.

كما نوهنا في الفصل السابق، يقوم سماسرة البيانات الضخمة بإنشاء قوائم مبوّبة لتصنيف لأفراد، مثل "القوقازيين ومثقفي الجامعات وسكان الأرياف ومحبي العائلة والمهتمين بالصيد والمهتمين بصيد السمك

ومشاهدة برنامج NASCAR (سباق السيارات)". يبدو الأمر الآن وكأن سماسرة البيانات ينشئون بدورهم قوائم تعود بأرباحٍ مباشرة على الجماعات الإجرامية المنظمة، والذين بدورهم يدفعون أعلى الأسعار مقابل مثل هذه الإرشادات الإجرامية. يمثل المحتالون بالبريد الإلكتروني منبعاً غزيراً للربح بالنسبة لسماسرة البيانات، وصناعة البيانات سعيدة بدورها بإنشاء قوائم تزود بها زبائن الإجراميين. ومع أن سماسرة البيانات سيعارضون وسيتملصون من أية مسؤولية عما يُفعل بتلك القوائم، فإن إنشاء فئات مثل "المتقاعدين عن العمل البسطاء الذين يرغبون في تصديق أن حظهم يمكن أن يتغير" ليس إلا دعوة لخداع المعمّرين للاستيلاء على مدخراتهم.

أما سماسرة البيانات، مثل تشويسبوينت وإكسبيريان وإيكويفاكس، فإن دوافعهم الاقتصادية أبعد ما تكون عن الاهتمام بشأن المخاطر المفروضة على العامة وعن المنظور الأمني للأمور. وهو ما يصح على نحو الخصوص في عصر البيانات الكبيرة، الذي يجد المجرمون المنظمون أنفسهم فيه منخرطين في مجال أعمال معتمد على إدارة المعرفة. وهم يشكلون قوة فعالة ومؤثرة وناشطة في عالم البيانات الكبيرة، وكلما أنتجنا بياناتٍ أكثر سعدوا أكثر باستهلاكها.

أمراض الشبكات الاجتماعية

تُعتبر الوسائط الاجتماعية مصدراً هاماً لسرقة الهويات، فكل ما يحتاج إليه مجرمو المعلومات لملاحقتك متوفر مجاناً على الإنترنت، سواء تاريخ ميلادك أم الاسم الثاني لوالدتك، كلاهما موجود على حسابك على الفايسبوك. وقد تظن أن "المجرمين لا يمكنهم رؤية معلوماتي لأنني قمت بمنع ذلك في إعدادات الخصوصية". كان ذلك سيصح لو أن النظام يعمل كما هو معلن. فثمة العديد من العوامل التي تجعل تسرب هذه المعلومات

الموضوعة على الفايسبوك ممكناً. أولاً، وكما أشرنا من قبل، عندما يقوم الفايسبوك بتحديث معايير وشروط الخدمة الخاصة به، فهو غالباً ما يعيد إعدادات الخصوصية التي قمت بتخصيصها بحسب رغبتك إلى أدنى حد ممكن من الخصوصية، ليجعل هذه البيانات متوفرة للجميع وخاصة المعلنين العاملين معه. ثانياً، ومع وجود 600,000 حساب على الفايسبوك يتم اختراقها يومياً، فإن وصول المجرمين إليك ليس سوى مسألة وقت. أخيراً، وبما أن البيانات الاجتماعية هي "مكمن المال"، فقد قام المجرمون بابتداع أدوات خاصة على شكل فيروسات مهاجمة للاستيلاء على حساباتك الموجودة على الفايسبوك وغيرها من مواقع التواصل الاجتماعي دون الحصول على إذن منك.

تعرض ما لا يقل عن 40 بالمئة من مستخدمي الوسائط الاجتماعية لأحد البرمجيات الخبيثة، وقد تعرض البريد الإلكتروني أو حساب التواصل الاجتماعي لأكثر من 20 بالمئة منّا للاختراق أو الاستيلاء من قبل طرفٍ ثالث دون إذن. فالأشرار يستجرّون المستخدمين للنقر على روابط موجودة في كتابات ورسائل يوهمونهم بأنها قادمة من أصدقائهم أو زملائهم بتطبيق تقنية تُسمّى الهندسة الاجتماعية. إذ يستفيد المجرمون من الثقة التي نقدمها لأولئك الموجودين على حساباتنا على الشبكات الاجتماعية بالتنكر الإلكتروني في هيئة الأشخاص الموثوقين، ليقوموا باستمرار باستدراج المستخدمين إلى النقر على رابط ينقل في النهاية فيروساً أو حصان طروادة أو دودة إلى الحاسب. علاوة على ذلك، فإن عصابات الجريمة المنظمة سريعة في استغلال الأخبار العاجلة التي تستخدمها في خداع المستخدمين الأبرياء، ودفعهم إلى النقر على روابط ذات صلة كوسيلةٍ لإصابتهم. فسواء كان الخبر العاجل متعلقاً بزلزال هاييتي أو باعتقال جاستين بيبر أو تعري ميلي سيروس، تتمتع هذه العناوين الرئيسية بجاذبية لا يمكن معها

تجاهلها، لذلك يقوم الناس بالنقر على روابطها. فعندما فُقدت الطائرة M التابعة للخطوط الجوية الماليزية فوق المحيط الهندي، كان المحتالون على أهبة الاستعداد لتقديم صور مزيفة عن الطائرة وفيديوهات مزعومة تُظهر "الطائرة موجودة في البحر، فيديو صادم تم بثه للتو على محطة سي.إن.إن". وكانت الرسائل تنتشر كالنار في الهشيم على مواقع التواصل الاجتماعي لتصل إلى الأشخاص الفضوليين التواقين إلى أجوبة عن الحادث، غير مدركين للفيروسات التي كانت تصيب أجهزتهم. فمن الفضول بالفعل ما قتل.

من أشهر نماذج الفيروسات الخبيثة التي تصيب مواقع التواصل الاجتماعي فيروس يُعرف باسم كوبفيس، وهو تحوير مقلوب لاسم فايسبوك، يستهدف مستخدمي الفايسبوك حول العالم. وتنتشر دودة الوسائط الاجتماعية الخبيثة هذه على مواقع التواصل الاجتماعي، من خلال خداع المستخدمين واستدراجهم للنقر على رابط موجود على الفايسبوك يحمل عنواناً مقنعاً جذاباً مثل "يا إلهي، لقد شاهدت للتو فيديو يظهرك وأنت عارٍ!". فمن منّا لن ينقر على مثل هذه الرسالة؟ لسوء الحظ، قد تقود نقرة فضولية واحدة منك إلى دفق من البرمجيات الخبيثة. وبمجرد الإصابة بدودة كوبفيس تقوم الأخيرة بسرقة أية بيانات دخول يمكن إيجادها على جهازك، ومن ضمنها تلك الخاصة بالفايسبوك والسكايب وياهو ماسينجر وجيميل. ويمكن لكوبفيس أيضاً أن يجبر حاسبك على الاشتراك في هجمات حجب الخدمة التي تُشنّ ضد أطراف أخرى وأن يسيطر على الفأرة لتقودك عبر نتائج البحث إلى مواقع غير موثوقة. تم تصميم البرمجية الخبيثة ونشرها على يد مجموعة قرصنة في مدينة بيترسبورغ الروسية، وبالرغم من معرفة هويات المجرمين المسؤولين ونشر أسمائهم، فإن السلطات الروسية رفضت تسليمهم للعدالة ليُحاكموا على

جرائمهم.

أصبحت أدوات الهجوم على مواقع التواصل الاجتماعي ممنهجة في أيامنا بالطبع، إذ لا يحتاج المرء لأن يكون قرصاناً محترفاً لكي يسرق المعلومات. ويمكن لأي شخص أن يحمّل برنامج فَيَرشيب على سبيل المثال، وهو إضافة برمجية لمتصفح فايرفوكس، للسيطرة على جلسة فايسبوك لآخرين على الشبكة نفسها وسرقة حساباتهم على الموقع. وهكذا، إذا كنتَ تعاين حسابك على الفايسبوك في مقهى ستاربوكس المحلي أثناء اشتراكك بالشبكة نفسها مع خمسةٍ وعشرين شخصاً على سبيل المثال، وكان أحدهم يشغل فَيَرشيب، فإن القرصان قادر على استخدام البرنامج للدخول إلى حسابك وكأنه أنت. الأمر في غاية السهولة، وحالما يتمكن من الدخول، يصبح باستطاعة المحتال رؤية جميع المعلومات المتعلقة بك وتغيير إعدادات حسابك وكتابة أي شيء يريده على حائطك أو في الرسائل المرسلة للمستخدمين الآخرين. تُسمى هذه التقنية سرقة الجلسة أو السرقة الجانبية ويمكن تنفيذها بسهولة بالغة.

يستهدف المجرمون المستخدمين على مواقع التواصل الاجتماعي بواسطة الألعاب الشبكية وتطبيقات من طرف ثالث أيضاً، حيث تمنحهم هذه الهجمات إمكانية الدخول إلى حسابك المصرفي وتدمير رصيدك. كان ذلك هو الدرس القاسي الذي تعلمته ليزا لوكوود من مدينة بالتيمور في ولاية ميريلاند الأميركية، عندما قام ابنها البالغ من العمر سبعة عشر عاماً بتقديم بعض المعلومات لتطبيق خاص بالألعاب على الفايسبوك سرعان ما عاد على كليهما بكارثة. وكانت اللعبة تعرض على الطفل نقاطاً أعلى أثناء اللعب مقابل ملء الطلب الخاص بالحساب، والذي يسأل عن رقم الضمان الاجتماعي. ودون تفكير، وبتخيل النقاط الأعلى التي تزيد مستواه في اللعبة وهي ترقص أمامه، قام الطفل بإتمام الطلب غير مدرك لحقيقة أن رقم

الضمان الاجتماعي الخاص به على وشك أن يُستخدم من قبل المجرمين ليتمّوا عن طريقه سبعة طلبات مستقلة لقروض سيارات في غضون أيام. ولم تعلم والدة الصبي بالحادثة إلا بعد أن تلقت اتصالاً هاتفياً من تاجر محلي لسيارات سوبارو فولكسفاغن يسأل فيه عن طلب القرض الذي تقدمّ به ابنها لشراء سيارة جديدة.

البيانات المسروقة: أساس انتحال الهوية

أدى الانفجار الذي تشهده حجوم البيانات إلى خلق صناعة جديدة لعصابات الجريمة المنظمة العابرة للحدود، تمثّلت في السرقة الواسعة للهويات. فوفقاً لخدمة الأبحاث التابعة للكونغرس، تكبد الأميركيون حوالى 2 مليار دولار عام 2012 نتيجة عمليات انتحال الهوية، ووقع أكثر من 13.1 مليون أميركي سنوياً، أي حوالى أميركي واحد كل ثانيتين، ضحايا لانتحال الهوية، وفقاً للتقارير. كما أن سرقة مثل هذه المعلومات المُحدِّدة للشخصية تشكل مدخلاً يقود إلى عدد من الجرائم الأخرى، مثل الاحتيال المالي والاحتيال على الضمان والضرائب والشؤون الاجتماعية والهجرة غير الشرعية بل وحتى تمويل الإرهاب. أي إن النمو الأسّي للبيانات يقود إلى نمو أسّي للجريمة الإلكترونية.

الأطفال هم أسرع مجموعات ضحايا انتحال الهوية نمواً. فهم غالباً ما يكونون أكثر عرضة للأذى، لأنهم لا يملكون أنظمة إنذار مبكر كالتي يمتلكها البالغون. فإذا احتال شخص ما وأدان بطاقتك الائتمانية بمبلغ 500 دولار أو 1000 دولار، فستلاحظ ذلك في كشف حسابك التالي على الأرجح، أما الأطفال فليس لديهم كشوف حساب لأرصدتهم. ويمكن للصوص الذين يسرقون هوياتهم أن يستخدموها لمدة ثماني عشرة سنة إلى أن يبلغ الأطفال ويتمكنوا من الدخول إلى أرصدتهم لطلب المال، مثل قروض طلاب الجامعات، ليعلموا حينها أن كشوف أرصدتهم قد دمّرها لصوص

المعلومات.

يقع في الولايات المتحدة لوحدها 500,000 طفل ضحية انتحال الهوية سنوياً. ووفقاً لدراسة قام بها المختبر الإلكتروني في جامعة كارنيج ميلون وشملت 40,000 طفل، فإن احتمال وقوع الأطفال ضحايا عمليات انتحال هوية هو أكبر بواحدٍ وخمسين مرة منه لدى البالغين، وهو رقم صادم. فابتداءً من الأطفال الصغار ووصولاً إلى المراهقين، يبقى اليافعون دائمي التعرض للاستهداف لعدم توفر كشوف لأرصدتهم، الأمر الذي يشكل نقطة انطلاق بالنسبة لعصابات الجريمة المنظمة. ولا يكتشف الآباء تلك الجرائم وعمليات انتحال الهوية سوى بعد سنوات وسنوات عندما يواجهون فجأة الجُباة العدوانيين الذين يريدون جباية ديون أطفالهم غير المسددة. ونظراً للمدى الذي يصله الأطفال والبالغون الصغار في حياتهم على الإنترنت، وللطرق الوحشية التي يتبعها سماسرة البيانات والشركات الكبرى في تتبعهم، ربما كان من المتوقع أن يواجهوا تهديدات كبيرة من منتحلي الهويات. وليت تلك المحن المالية كانت أكبر مشكلة تواجههم. فكما سنرى، قد تقود البيانات التي نسربها إلى مخاطر جسدية أيضاً.

المُطاردون والمتنمرون والعلاقات السابقة - يا إلهي!

لا تُستَغَل كميات البيانات التي تفيض من حولك على الإنترنت من قبل لصوص الهويات وحدهم، فأعداد هائلة من المجرمين تستفيد منها أيضاً. ومع الوقت، تصبح الجرائم المعروفة في عالم الأمس ممكنة أيضاً في إطار التقنيات الأكثر حداثة، والبيانات الكبيرة تسمح للمجرمين التقليديين بمهاجمتك بدقة لا تنفك تزداد. فمن خلال وجودنا المستمر على الإنترنت على مدار الساعة، يمكن الوصول إلينا في أي وقت، حتى من قبل أولئك الذين لا نرغب بوصولهم إلينا. والغريب في هذه الظاهرة هو أننا في أحيانٍ كثيرة، ومن خلال مخزون المعلومات الذي نقدمه طوعاً عن أنفسنا أو عن

طريق بياناتنا المسرّبة، نعبّد الطريق أمام المطاردين والمتحرّشين والمجرمين لكي يصلوا إلينا.

ولنأخذ مثلاً حالة التنمّر السايبري. فبالرغم من أن التنمّر لطالما كان مشكلة في المدارس، فإن الإنترنت تزود المتنمِّرين السايبريين بإمكانية الوصول المباشر إلى ضحاياهم، ليس فقط في باحة المدرسة، بل في كل مكان وزمان. وتأتي التهديدات على الإنترنت عن طريق البريد الإلكتروني ومواقع التواصل الاجتماعي والهواتف النقالة، وحتى عن طريق تطبيقات الرسائل والألعاب. فوفقاً للمجلس الوطني للوقاية من الجرائم، يتأثر نصف المراهقين تقريباً بالتنمّر السايبري. ويبدو الأمر بالنسبة للشبان الذين يواجهون مضايقة مستمرة وكأنه لا مفر منه؛ وهو ما يفسّر اعتراف 20 بالمئة من طلاب المدارس المتوسطة "بأنهم يفكرون جدياً بالانتحار" بسبب التنمّر على الإنترنت.

ليس الأطفال هم وحدهم من يقع ضحية التنمّر الإلكتروني، فالملاحقة السايبرية تستهدف البالغين أيضاً وعلى نحو متزايد. في الحقيقة، فإن هذا التدفق المتنامي بلا توقف للبيانات المتعلقة بنا وبحضورنا المستمر على الإنترنت، ساعد على تحويل الإنترنت إلى بيئة خصبة لنوع جديد من المجرمين يُعرف باسم المطاردين الإلكترونيين. ويستخدم هؤلاء المهاجمون الإنترنت "كسلاحٍ لهم لمضايقة وتهديد وإخافة فريستهم". ويقوم المطاردون الإلكترونيون بذلك عن طريق إرسال رسائل إلكترونية أو نصية أو كتابات أو تغريدات غير مرغوبة، وكذلك عن طريق نشر الإشاعات عن ضحيتهم على الإنترنت. باستخدام البيانات التي نسربها كل يوم، أو تلك التي يوفرها سماسرة البيانات، يمكن للمطاردين الحصول وبسهولة على معلومات مفصلة عن ضحاياهم، بما فيها عناوين منازلهم وأماكن عملهم وأرقام هواتفهم. وغالباً ما يستخدم المطاردون هذه البيانات لمواجهة ضحاياهم

شخصياً.

كانت للفايسبوك فائدة خاصة بالنسبة للمطاردين. فمع امتلاك كل منا مئات الأصدقاء، كثيرين منهم لم نقابلهم على الإطلاق، من الحكمة أن نفكّر ملياً بهوية من يرسل طلبات الصداقة تلك. فقد استخدم كريستوفر دانيفيغ الفايسبوك للعثور على ضحيته، وكانت فتاةً في الثامنة عشرة من عمرها من مدينة سدني في أستراليا اسمها نونا بيلوميسوف، وقام بدراسة حسابها بدقة قبل أن يتصل بها. وقد أسهمت الكتابات المستمرة لبيلوميسوف على صفحتها على الفايسبوك عن حبها للحيوانات، في إلهام مُطاردها بطريقة لإقناعها بمقابلته. فباستخدام البيانات التي كانت الفتاة الشابة تسربها ببراءة على مواقع التواصل الاجتماعي، أنشأ دانيفيغ حساباً وهمياً على الفايسبوك تحت اسم "جيمس غرين" وزعم أنه المسؤول عن التعيين في مجموعة محلية مشهورة لإنقاذ الحيوانات. واستخدم المُطارد أدق التفاصيل التي كتبتها ليتمكن من خداعها. فبعد إنشاء الحساب المزيف، اتصل دانيفيغ ببيلوميسوف وتبادل معها سلسلة من الرسائل، وفي النهاية حصل على صداقتها ونال ثقتها. وبعد ذلك بوقت قصير، أعلن أن هنالك فرصة عمل على وشك أن تتاح في مؤسسة خيرية لإنقاذ الحيوانات، مدعياً أن العمل يناسبها تماماً. فوافقت الفتاة على لقائه لإجراء مقابلة معه، ثم عرض مطاردها أن يقودها إلى مأوى للحيوانات يقع في منطقة منعزلة في ضواحي سدني. ووافقت الفتاة على اقتراحه بالسفر معه مدفوعة بحماستها لإمكانية العمل في مكانٍ مأجور يضم الحيوانات التي لطالما أحبتها. وهناك، في ضواحي مدينة سيدني، قام دانيفيغ بخنق الفتاة وقتلها.

مع أن التهديد الصادر عن الغرباء الذين يستخدمون بياناتنا للعثور علينا ومطاردتنا هو تهديد حقيقي، فإنه يبدو باهتاً إذا ما قورن بالمخاطر التي نواجهها نتيجة العنف المنزلي والأذى الذي يسببه من كانت تجمعنا به

علاقة حميمة. يُسهّل الفايسبوك الاستمرار في مراقبة صديق سابق أو صديقة سابقة أو طليق أو طليقة بدافع من مستوى طبيعي، ولو كان غير صحي، من الفضول صعب الإرضاء. فالأصدقاء الجدد وتطورات الحياة والتغيرات في حالة العلاقات ومواقع السفر وخطط الإجازات، كل ذلك مهم جداً بالنسبة للشركاء السابقين. وهي ظاهرة شائعة إلى حد أن "المطاردة على الفايسبوك" دخلت إلى القاموس العام.

لكن البيانات التي نسربها تثير لدى البعض ما هو أكبر بكثير من مجرد فضول الشركاء السابقين. فقد اعترف 45 بالمئة من ضحايا العلاقات التي تتضمن عنفاً منزلياً في العالم المادي، بأنّ من آذاهم قد قام بملاحقتهم والهجوم عليهم على الإنترنت مسبباً للكثيرين المعاناة من متلازمة ما بعد الرض. ويمكن للبيانات الاجتماعية أن توفر تفاصيل مرتبطة بالموقع الجغرافي، ولأن هؤلاء المُؤذين غالباً ما يتجاوزون كل الحدود في ملاحقة ضحاياهم، فإن تغريدة بريئة أو تسجيل دخول في أحد المواقع أو تحديث حالة على موقع آخر يمكن أن يعادل في خطره خطورة الرصاصة. وقد سافر بول بريستول على سبيل المثال بالطائرة من ترينيداد إلى إنكلترا ليطعن صديقته السابقة حتى الموت بعد رؤيته لصورة لها مع صديقها الجديد على الفايسبوك.

ثمّة تحدٍّ آخر في عالم البيانات الكبيرة، يتمثل في كون معلوماتنا التي نشاركها، معتقدين أنها ستبقى خصوصية، تتسرب إلى الآخرين. فغالباً ما نتعرض للخيانة من قبل أولئك الذين وضعنا في عهدتهم أدق التفاصيل الحميمة في حياتنا، وخاصة في موضوع الصور التي قمنا بمشاركتها. فالجنس عبر الرسائل، أو مشاركة الصور الجنسية الصريحة عبر الرسائل القصيرة عن طرق الهواتف النقالة، هي ظاهرة متنامية، وقد اعترف 67 بالمئة من طلاب الجامعات البالغين بأنهم تورطوا في هذه المسألة. ولسوء الحظ، فإن الصور

التي تتم مشاركتها بهذه الطريقة لا تختفي تماماً. وهذا الشكل من تشتت البيانات كغيره من الأشكال السابقة، غالباً ما يعود لينغّص على من أصدرها بطرق غير متوقعة.

هنالك مواقع مثل MyEx.com تسمح للأشخاص المنبوذين بمشاركة صور عشاقهم السابقين على موقع واحد. وثمة أكثر من سبعمئة صفحة تضم صوراً لرجال ونساء عراة، مع فقراتٍ من التشكّي ممن في الصور، هذا العاشق الرهيب ذو القضيب الصغير، كان يخونني مع أختي. وهناك موقع آخر اسمه IsAnyoneUp.com، أنشأه رجل عمره أربعة وعشرون عاماً واسمه هانتير مور كمستودع بيانات يَسمح لأي شخص بوضع صورٍ لشركائه السابقين أو لأعدائه وهم عراة، وكان الموقع يستقبل ربع مليون شخص يومياً. وقد شاعت هذه الظاهرة وصار لها اسم الآن: الإباحية الثأرية. صُمم موقع مور بحيث يضع بجانب كل صورة روابط لحسابات الشخص المستهدف على الفايسبوك وتويتر واسمه الكامل واسم مدينته، وجعلت هذه المعلومات مفهرسة وقابلة للاسترجاع من قبل غوغل بحيث تظهر في أي وقت يتم فيه إجراء بحث بريء عن الشخص المعني من قبل طرف آخر. كانت كل صورة عارية مرفقة بقسم للتعليقات يسمح للعامة ولمور نفسه، بالتعليق على هذه الصور والسخرية منها.

التهديدات الإلكترونية للقاصرين

وفقاً لمركز بيو للأبحاث، فإن 95 بالمئة من الشباب في الولايات المتحدة متصلون بالإنترنت اليوم، و74 بالمئة من المراهقين الذين تتراوح أعمارهم بين اثنتي عشر عاماً وسبعة عشر عاماً يستخدمون الإنترنت عن طريق هواتفهم النقالة، إذ غالباً ما يدخلون إلى عالم الإنترنت عن طريق هواتفهم الخلوية وحواسبهم اللوحية. علاوةً على ذلك، يقتني 95 بالمئة من الشبان الذين تتراوح أعمارهم بين عشرة أعوام وثلاثة وعشرين عاماً حساباً واحداً

على مواقع التواصل الاجتماعي على الأقل. والكثير من عمليات الدخول إلى الإنترنت يتم خارج نطاق الأهل، الذين يقول 74 بالمئة منهم إن التقانة الحديثة تغلبت عليهم وإنه لم يعد لديهم الطاقة أو الوقت أو القدرة لمراقبة ما يفعله أولادهم على الإنترنت. إنه أمر مؤسف، فمع أن التنمّر الإلكتروني من قبل الأصدقاء هو سبب رئيسي للضغط النفسي عند الشبان، إلا أنهم يواجهون مخاطر أعظم بعد في عالمنا الذي يزداد تواصلاً.

يستخدم صائدو الأطفال التقانة بفعالية كبيرة للتركيز على الأطفال لأغراض العنف الجنسي. وهي ممارسة شائعة إلى حد أن برنامجاً تلفزيونياً يلقي الضوء على هذه الظاهرة، هو برنامج لنمسك صياداً على محطة إن.بي.سي. أما التحدي الذي يواجه الأطفال فيكمن في كون أربعة من أصل كل خمسة أطفال لا يمكنهم أن يكتشفوا أثناء الحديث على الإنترنت أن من يتكلم معهم هو شخص بالغ يتظاهر بأنه طفل. فصديقهم الجديد على الإنترنت، وهو فتاة عمرها ثمانية أعوام من بلدة مجاورة، لا يستبعد أن يكون رجلاً في الخمسين على بعد ولايتين مستعداً للسفر عبر حدود الولاية بهدف اختطاف طفل.

نظراً لوجود تفضيلات واضحة لدى البيدوفيليين يسعون وراءها لدى الأطفال الذين يطاردونهم (مثل العمر والجنس ولون الشعر والطول وغير ذلك)، فإن أية صورة توضع على مواقع التواصل الاجتماعي أو في أي مكانٍ آخر على الإنترنت يمكن استخدامها مثل دليلٍ للتسوق، أو كسوقٍ حقيقية بالنسبة للأشخاص المستغلين للأطفال والباحثين عن ضحايا يستهدفونها. وينكبّ البيدوفيليون على تعرّف أحدث الألعاب وخدمات الرسائل والعوالم الافتراضية المشوقة للأطفال، وهم يبحثون عن ضحاياهم في أي ميدانٍ ممكن على الإنترنت، مستخدمين أدوات متنوعة تبدأ بأجهزة إكس بوكس وتنتهي بأجهزة آيباد. وإذا كنت تظن أن الطلب على مثل هذه الصور

المقلقة محدود، فقد تعرفت مصادر السلطة التنفيذية ما لا يقل عن اثنين وعشرين مليون صورة وفيديو مشابهة في الولايات المتحدة وحدها، وارتفع أعضاء بعض المواقع الإباحية الطفولية المحمية بكلمة سر ليصل إلى ثلاثين ألف عضو مُسدِّد.

في وقتنا هذا، تتكاثر صور الأطفال الإباحية، ليس بالضرورة لأن شخصاً بالغاً قد قام باختطاف طفل واستغلاله، بل نتيجة استهداف اليافعين باستمرار بالخداع والهندسة الاجتماعية.

تلك كانت حالة أماندا تود من مقاطعة بريتيش كولومبيا في كندا، عندما كانت في سن الثانية عشرة حين أُجبرت على تصوير مقطع فيديو لصدرها على موقع للمحادثة المباشرة معروف بين المراهقين هو موقع BlogTV. أما الشخص المجهول الذي طلب ذلك فكان يبدو لطيفاً، حيث قام بمجاملة أماندا الفتية والإثناء على جمالها. وفي لحظة مراهقة ساذجة، كشفت أماندا عن صدرها مفترضة أن صاحب الطلب كان مراهقاً آخر. ومع مرور الوقت، أدركت أنها كانت تواجه قوة أكثر شراً. فبعد سنة على ظهورها وهي عارية، تلقت أماندا رسالة على الفايسبوك من رجل يحمل اسماً مستعاراً طلب منها أن تظهر مجدداً وهي عارية وأن تقوم بحركات جنسية على الكاميرا من أجله. وقد هددها في حال رفضها بإعادة نشر الفيديو الأصلي الذي يظهرها عارية الصدر. ولكي يثبت لها أنه كان جاداً في تهديده، قام المهاجم بكشف أسماء أصدقاء أماندا وعائلتها وعنوانها والمدرسة التي تذهب إليها وقال إن الجميع سيشاهدون الفيديو الخاص بها. لكن أماندا تمنّعت، وهنا بدأت المضايقة.

أنشأ الشخص المضايق حساباً مزيفاً على الفايسبوك يحمل اسم أماندا واستخدم صورة صدرها العاري كصورة للحساب. بعد ذلك بدأ بإرسال طلبات صداقة لجميع أصدقاء أماندا وأفراد عائلتها وأساتذتها الذين حصل

عليهم من حسابها الحقيقي. ولم تدرك أماندا ما يحدث إلى أن جاءت الشرطة، قلقة من تبعات الحادثة، وقرعت باب عائلتها في الساعة الرابعة صباحاً من ليلة عيد الميلاد. شعرت أماندا بالهلع. وبعد عودتها إلى المدرسة، تعرضت للتنمّر والإزعاج بقسوة. وأصبح الضغط لا يُطاق بالنسبة للمراهقة الصغيرة التي دخلت حالة من الاكتئاب والقلق والذعر. فكانت في كل ليلةٍ تبكي إلى أن تنام، بينما تخلى عنها أصدقاؤها الذين كانوا يلومونها على ظهورها في الفيديو. وباتت تأكل وجبة الغداء لوحدها كل يوم وبدأت تجرح نفسها.

تجنباً للألم والسخرية، غيّرت أماندا المدرسة وانتقلت إلى بلدة أخرى. لكن لسوء حظها، لم تتوقف الملاحقة. فقد تابع مُطاردها نشاطاتها على الإنترنت وأنشأ صفحة جديدة على الفايسبوك لينصح أساتذتها وزملاءها الجدد بمشاهدة فيديو صدرها العاري. وفي المدرسة الجديدة، كان تنمّر الصف عليها في غاية القسوة إلى حد أن مجموعة من الفتيات هاجمتها في الباحة وضربتها ومرغتها في حفرةٍ موحلة. إضافة للإهانة والأذية، قامت المعتديات بوضع فيديو الهجوم على الفتاة على اليوتيوب. وحين عادت أماندا إلى المنزل في تلك الظهيرة شربت من عبوة مادة مبيضة في محاولة منها لوضع حدّ لألمها ومعاناتها، لكنها أسعفت إلى المستشفى حيث غسلت معدتها. ومع أن أماندا قد نجت، فإن المضايقة قد استمرت. فقد قام طلاب آخرون بوضع صور لحاويات الكلوروكس على صفحتها على الفايسبوك وشجعوها على "بذل جهد أكبر في المرة القادمة". رداً على ذلك، وفي السابع من أيلول عام 2012، قامت تود بوضع فيديو مدته تسع دقائق على اليوتيوب لتشرح بالتفصيل صراعها مع التنمّر والأذى الذي لحق بها. وفي هذا الفيديو المؤثر جداً، قامت أماندا بمشاركة تجاربها المتعلقة بالمضايقة التي تعرضت لها، مع موسيقى مؤثرة في خلفية الفيديو. وبعد ذلك بوقت قصير، أصبح من

المستحيل بالنسبة لأماندا احتمال الألم، فقامت بالانتحار في سن الخامسة عشرة.

أصبح الفيديو الخاص بأماندا فيروسياً بعد موتها فشاهده الملايين في ذلك الوقت. واعتقد بعض أفراد الشرطة أن أماندا قد تكون ضحية لما يُسمّى مستغلي الفيديوهات، وهي نزعة مزعجة تقوم من خلالها عصابات البيدوفيليين على الإنترنت بالاستمتاع عن طريق إجبار الأطفال على التعري أمام الكاميرات وتصويرهم. والأسوأ من ذلك هو أن هؤلاء المستغلين يستخدمون الفيديوهات لابتزاز المراهقين لكي يقوموا بأنفسهم بحركات جنسية صريحة على الإنترنت. إن قضية أماندا تود متعددة الوجوه. إذ قامت الفتاة اليافعة بسذاجة بتسريب بيانات خاصة بها على الإنترنت، وتمت مطاردتها على مواقع التواصل الاجتماعي وفي العالم الحقيقي، مما أدى إلى مصرعها. وعلى الرغم من مأساوية الحدث، فإنه ليس حدثاً منعزلاً، بل هي نزعة تتنامى بمعدل يثير القلق. تؤدي البيانات الكبيرة إلى مخاطر كبيرة، وحتى المعلومات التي تتم مشاركتها ببراءة من قبل البالغين يمكن أن تستخدم من قبل مستغلي الأطفال.

ففي عام 2011، اكتشفت الشرطة في مدينة ميلبورن الأسترالية عدداً من المتحرشين بالأطفال يستهدفون الأمهات الوحيدات مع بناتهن، وذلك عن طريق اصطياد حساباتهن على الإنترنت والبحث عن إشارات إلى أولادهن. وكان هدف هؤلاء البيدوفيليين هو شق طريقهم نحو منزل الضحية، حيث كانوا يستخدمون اسماً ومظهراً مستعاراً، في محاولة للبدء بعلاقة مع والدة الطفل. وحين تتم دعوة أحدهم إلى المنزل واستقباله فيه، يقوم باستثمار الوقت الذي يكون فيه وحيداً في المنزل ليستهدف بنت الأم العازبة. يلعب المجرمون والمتصيّدون وفقاً لقواعد مختلفة، ويسعدهم استخدام جميع بياناتنا كمصدر تغذية، وهو أمر له عواقب متنوعة غير سارة.

وسيكره الحاقدون

قد يجعلك حسابك على مواقع التواصل الاجتماعي عرضة لنوع آخر من الهجمات، هو جرائم الكراهية التي يقوم فيها المتعصبون والعنصريون باستهداف الأفراد على الإنترنت، بناءً على عرقهم أو ديانتهم أو عقيدتهم أو لونهم أو جنسهم أو ميولهم الجنسية. وقد وقعت مثل هذه الحوادث على مواقع مثل فايسبوك وأنستاغرام وآي.سي.كيو وتويتر وغيرها من مواقع التواصل الاجتماعي. بل إن فايسبوك اتُّهم باستضافته للكثير من محادثات الكراهية، إلى حد أن محطة سي.إن.إن بثت سلسلة عنوانها "فايسبوك/هيتبوك؟"، أو الفايسبوك:كتاب الكراهية، لتوثق هذه الظاهرة.

تسمح البيانات الموجودة على الإنترنت للمجرمين باختيار ضحاياهم وفقاً للتوجهات الفردية للمهاجم. فذات مرة، استهدف معتد في تكساس رجلاً غير سوي جنسياً قابله على موقع MeetMe.com للتواصل الاجتماعي. وبعد أن رتب المهاجم لقاءً مع الضحية قام باختطافه وضربه حتى أغمي عليه ثم قيّد معصميه ووضعه في صندوق سيارته ليلقيه على قارعة الطريق. وأدين برايس جونسون من مدينة فورت وورث بالهجوم، وحين تم اعتقاله قال إن كل ما كان يريده هو أن يلقّن الرجل درساً، لكنه اعترف بأن "المزحة ربما تجاوزت حدها".

بقدر ما كانت حادثة تكساس مرعبة، فإن حجم جرائم الكراهية على مواقع التواصل الاجتماعي في الولايات المتحدة يُعتبر تافهاً بالمقارنة مع ما يجري في روسيا، حيث تنسب الآلاف من الهجمات إلى حركة النازية الجديدة الناشئة في البلاد. ففي برنامج وثائقي مدته ساعة من إنتاج القناة الرابعة الإنكليزية، يقوم المراسلون بتوثيق أكثر من ألف وخمسمئة حالة اختطاف، حيث تقوم مجموعات أهلية باصطياد الشبان في الشوارع وعلى الإنترنت. أما الضحايا، وجلّهم من المراهقين، فيتم اختطافهم والاعتداء

عليهم وإرهابهم أثناء اختطافهم، وغالباً ما يتم تصوير ذلك بكل جرأة، إذ لا يخشى هؤلاء المهاجمون عقاب الشرطة المتواطئة في العملية، ولذا فإنهم يقومون بوضع الفيديوهات التي تظهر هجومهم الوحشي على مواقع الفايسبوك وأنستاغرام، في محاولةٍ منهم للإمعان في إذلال المتضررين. وبالرغم من الأدلة الكثيرة الموجودة على الإنترنت والتي توثق لمئات الحالات، فإنه لم تُسجّل أية حالات اعتقال أو ملاحقات قضائية حتّى عندما يتم قتل الضحايا أو تركهم مع إعاقات دائمة، في تناقض غريب مع ما نعرفه من قدرة الشرطة الروسية على المراقبة المنهجية لكل نشاطات الإنترنت في البلاد من خلال قنوات التواصل الاجتماعي.

السطو في إصداره الثاني

هل سبق لك أن ذكرت على الفايسبوك عفواً إجازة قريبة لك؟ مفاجئ هو العدد الكبير من الناس الذين يتحدثون عن خطط سفرهم المستقبلية على الإنترنت، فيعبرون عن تلهفهم للقيام برحلة إلى عالم ديزني أو لقضاء عطلتهم على الشاطئ. أما ما لا يدركه هؤلاء فهو أن المجرمين قادرون على جمع هذه البيانات من الإنترنت واستخدامها لأغراضهم الشخصية (تذكر قانون غودمان: بقدر ما تنتج وتخزن من البيانات، تكون الجريمة المنظمة سعيدة باستهلاكها).

كان اللص في الماضي عندما يريد أن يسطو على منزلٍ معين يبحث بشكلٍ تقليدي عن أدلة واضحة على أن سكان المنزل في إجازة، كوجود كومة من الصحف أمام المنزل أو ضوء شرفة يبقى مطفئاً في الليل. لكن حتى اللصوص طوروا وسائلهم وبدأوا يوظفون التقانة على نحو متزايد للعثور على أهدافهم وعلى الممتلكات التي سيسرقونها. أهلاً بكم في عالم السطو في إصداره الثاني. حيث يواظب اللصوص اليوم على البحث عن كل ما تكتبه على الفايسبوك وغوغل بلَس وتويتر ويستخدمون البيانات التي تسربها

لتوجيه عملياتهم، تماماً كما يفعل أي تاجر أو مراقب. ولتسليط الضوء على هذا التهديد، قامت مجموعة هولندية من مطوري الحواسب الذين تقلقهم مبالغتنا في مشاركة البيانات بإنشاء موقع إلكتروني اسمه Ple (أو اسرقني أرجوك). حيث يقومون في هذا الموقع بجمع بيانات الموقع الجغرافي من خلال تغريدات الناس وتسجيلاتهم في موقع فورسكوير وتنظيمها في قاعدة بيانات قابلة للبحث. وكانت النتيجة هي أن اللصوص أصبح بإمكانهم التحري من خلال الرمز البريدي عن الأشخاص الغائبين عن منازلهم وعن مدة غيابهم وعن إمكانية السطو على منازلهم. أي إن اختيار الهدف الإجرامي يتم بنقرة من الفأرة.

ليس هذا التهديد أمراً فرضياً وحسب، فاللصوص في العالم المادي يقومون بالفعل بمراقبة البيانات الاجتماعية. ومثال ذلك ما حدث عام 2010، عندما قامت عصابة محلية من المجرمين من مدينة نَشوا بولاية نيو هامبشير باللجوء إلى الفايسبوك لتحديد الوقت الذي يكون فيه ضحاياها خارج المنزل. واكتشفت شرطة نَشوا أن هذه العصابة كانت تتفقد تحديث الحالات التي تطرأ على حسابات الضحايا قبل التنفيذ في أكثر من خمسين عملية سطو، تمثل فترة نشاطها سطت عبرها على ممتلكات بقيمة تبلغ حوالى 200,000 دولار. ليس هؤلاء اللصوص هم اللصوص ذاتهم الذين كانوا أيام جدك، فالمجرمون يتكيفون بسرعة مع التقنيات التي تساعدهم في ارتكاب المزيد من الجرائم. ووفقاً لدراسة تمت عام 2011 وطالت لصوصاً مدانين في إنكلترا، اعترف 78 بالمئة منهم بمراقبة الفايسبوك وتويتر وفورسكوير قبل تحديد المنزل المناسب للسرقة. كما اعترفوا أيضاً باستخدام أدواتٍ مثل غوغل ستريت فيو ليعاينوا المكان مسبقاً، وليخططوا مسار الهرب عند مغادرة مسرح الجريمة. تلقي النتائج الحاصلة الضوء على الطرق التي يمكن للمجرمين بواسطتها استخدام البيانات التي نسربها

ضدنا.

هناك طريقة أخرى يمكن للصوص استخدامها في هجومهم عليك، وهي بيانات المواقع المضمّنة في الملفات التي تضعها على الإنترنت. فكما نوهنا من قبل، تدمج تلك البيانات التي تسمّى البيانات الواصفة بشكلٍ خفي في الصور والفيديوهات وتحديثات الحالة التي تقوم بمشاركتها بواسطة هاتفك النقال، وهي تكشف تاريخ ووقت التقاط الصورة والرقم التسلسلي للهاتف أو الكاميرا، إضافة إلى، وهو الأهم، خط الطول وخط العرض (أي الموقع الجغرافي من خلال نظام تحديد المواقع العالمي جي.بي.إس) اللذين يحددان المكان الذي التقطت فيه الصورة. هذه البيانات الواصفة التي تحتوي على المعلومات، وإن تعذّرت ملاحظتها مباشرة عند مشاهدة فيديو أو صورة، متوفرة ومن السهل الوصول إليها من قبل أي شخص يعرف كيف يحمّل برمجية إضافية بسيطة للمتصفح قادرة على قراءتها. فباستخدام أي من هذه الأدوات المجانية التي تعدّ بالمئات، يمكن لصورك أن تبصر النور فجأة لتظهر على خريطة على غوغل مابس وكأن في الأمر سحراً، ما يسمح لأي شخص بتكبير الخريطة حتى يحدد بدقة الموقع الذي التقطت فيه الصورة. هذه هي معجزة الإكساء السايبري، أي استخدام المرء لبيانات الموقع الجغرافي المخفية لكي يخطط لجرائمه.

تتوفر هذه البيانات الواصفة نفسها في الملايين من الصور المنشورة على مواقع البيع والمزادات مثل قائمة كريغ وإي.باي. فعند وضع صورة لخاتم ألماسي أو لجهاز آيباد على موقع قائمة كريغ على سبيل المثال، قد تشتمل الصورة على الموقع الدقيق لمنزلك الذي التقطت فيه الصورة. وهي معلومات من شأنها السماح للصوص ذوي الخبرة التقانية باستخدام موقع قائمة كريغ كأنها دليل تسوق يظهر البضائع التي ستتم سرقتها قريباً.

عندما قرر كل من كيري مك.مولين وكورت بيندلتون من مدينة نيو ألباني

في ولاية إنديانا بيع تلفاز البلازما ونظام الستيريو لديهما، وضعا صوراً لهذه الأشياء على الإنترنت. وبعد عدة أيام، ذكر الزوجان على الفايسبوك أنهما سيحضران حفلة في مدينة لويسفيل المجاورة في ليلة ذلك السبت. فكانت تلك المعلومات هي كل ما احتاجه اللصوص للسطو على المنزل الذي يحتوي الأجهزة الإلكترونية التي كانوا يبحثون عنها. وكان اللصوص يعرفون أن لديهم الوقت الكافي للقيام بعملهم، لأن الحفلة ستمتد لساعات. وفي النهاية، سرق من الزوجين تلفازهما ذو الشاشة المسطحة وحاسبان محمولان وجهاز ستيريو مع كافة مكوناته وكاميرا رقمية عالية الدقة. وما هذه سوى واحدة من الطرق التي يمارس من خلالها المجرمون التجارة الإلكترونية، حيث يتم الإكساء الإلكتروني لمنزلك من الداخل بواسطة البيانات التي تسربها.

الاحتيال والقتل الموجّهان

ثمة طريقة أخرى يستفيد من خلالها المجرمون من كتاباتك المتعلقة بإجازتك أو تحديثات حالات السفر، وهي خداع أجدادك. نعم، يقوم المجرمون بمراقبة حساباتك على مواقع التواصل الاجتماعي ويشاهدون الصور التي تضعها على الإنترنت عن عطلتك في الوقت المناسب. وحالما تفعل ذلك، يقوم المحتالون بتحليل حساباتك على مواقع التواصل الاجتماعي ليبحثوا عن أقاربك الأكبر سناً، وعادة ما يكونون الجد أو الجدة، ليقوموا بإعلامهم عن تعرضك لحادث مؤسف. تجري الخدعة على النحو التالي: "مرحباً، الجدة؟ نعم، لدي أخبار سيئة. تعرض حفيدك بيتر لحادث فظيع في باربادوس. رفضت المستشفى تأمينه الأميركي وكذلك علاجه قبل أن ندفع 10,000 دولار للعملية الجراحية. إذا لم توافقي على دفع المبلغ، فلن يتم إجراء العملية". كيف يفلت المجرمون من العقاب على هذا الأمر؟ بمساعدتنا، ولو بدون قصد، عن طريق المعلومات التي نشاركها في عالم

البيانات الكبيرة الجديد هذا. يخبر الفايسبوك العالم بأسره، والجريمة المنظمة كذلك، بهوية أجدادنا بدقة وكيف يمكن العثور على العمة الطيبة مارغريت للضغط عليها: "يبدو الأمر سيئاً... دخل بيتر في غيبوبة... أرجوكِ أرسلي النقود حالاً!". وقد وقع المئات ضحية للسلب بهذه الطريقة وتم تحويل ملايين الدولارات عن طريق ويسترن يونيون وموني غرام نتيجة لذلك.

بينما قد تكلفك مراقبة مواقع التواصل الاجتماعي من قبل المحتالين بضعة آلاف من الدولارات، فإن ملاحقتك من قبل تجار المخدرات على تويتر قد تكلفك حياتك. إذ تعمل عصابات تجارة المخدرات على تطوير مجموعة واسعة من برامج الاستخبارات المضادة لجمع البيانات من مواقع التواصل الاجتماعي والمدوّنات وسلاسل المعلومات السرية الحكومية كوسيلة للكشف عن التهديدات المحتملة.

يتم التعامل بسرعة مع التعليقات التي تنشر على الإنترنت إذا كانت تصب في غير مصلحة عصابات تجارة المخدرات. ففي أيلول من عام 2011، تنبّه المواطنون على الطرف الآخر من حدود تكساس في منطقة نويفو لاريدو المكسيكية وهم في طريقهم إلى عملهم، إلى جثتين مقيدتي الأرجل والأذرع ومعلقتين فوق معبر للمشاة. كانت الضحيتان، وهما رجل وامرأة في العشرينيات من العمر، قد تعرضتا لتعذيب وحشي، بل كان قد تم انتزاع أحشاء المرأة بالكامل. وفوق الجثتين المتدليتين كان هناك تحذير مشؤوم واضح وتوقيع ضخم: "هذا هو مصير كل الواشين على الإنترنت... احذروا فإننا نراقبكم..". أما التوقيع بحرف زد فهو إشارة إلى جماعة زيتاز، وهي من أضخم وأعنف عصابات المخدرات في المكسيك. تتمتع هذه العصابات بالخبرة في حملاتها على مواقع التواصل الاجتماعي، حيث تقوم بتحميل الصور والفيديوهات على الفايسبوك وتويتر مستعرضة فيها قطع رؤوس

ضحاياها بالمناشير والخناجر.

في هذه الأثناء، لا يكتفي الإرهابيون باستغلال مواقع التواصل الاجتماعي من أجل تنفيذ عملياتهم وحسب، بل إنهم، كما رأينا في مومباي، يغردون بالزمن الحقيقي لتوجيه الرأي العام وإشاعة المزيد من الخوف بين أهدافهم. فخلال الهجوم على مجمع ويستغيت التجاري في نيروبي عاصمة كينيا في أيلول عام 2013، قام أعضاء جماعة الشباب التي نفذت العملية بالتغريد على موقع تويتر من داخل المجمع لنقل مجزرتهم على الهواء مباشرة. وقام الإرهابيون الذين يتخذون في الصومال مقراً لهم، بقتل ثلاثة وستين مدنياً بريئاً وجرح حوالى مئتي شخص آخرين. وقامت المجموعة أيضاً بوضع صور لهذه المجزرة من داخل مجمع على موقع تويتبيك ويستغيت متهمة الحكومة الكينية وحدها بتدمير مركز التسوق مستخدمين هاشتاغ #ويستغيت.

آثار الاستخبارات المضادة على البيانات الحكومية المسربة

تستخدم منظمات تجارة المخدرات والجريمة المنظمة، مواقع التواصل الاجتماعي لجمع معلومات استخبارية عن موظفي الحكومة والسلطة التنفيذية. فعندما قام نائبا الشريف في منطقة ماريكوبا كاونتي في ولاية أريزونا على سبيل المثال، باستيقاف سيارة للتحقق من القيادة تحت تأثير الخمر عام 2010، كشف البحث في السيارة عن وجود عدة أقراص مضغوطة تحمل بيانات تشتمل على أسماء وصور وحسابات فايسبوك لحوالى ثلاثين حارساً وضابطاً سرياً. كما تسعى الأطراف غير الحكومية وجماعات الناشطين - القراصنة مثل أنونيموس ولولزسيك وراء البيانات الاجتماعية المسربة من الموظفين الحكوميين.

في حادثة تعود إلى عام 2012، برهنت جماعة لولزسيك عن قوتها في مطاردة مكتب التحقيقات الفدرالي. فبعدما بدأت المنظمة بالتجسس على

عناوين البريد الإلكتروني الشخصية لأفراد الشرطة، خاصة أولئك العاملين في مجال الجريمة السايبرية، باتت قادرة على اعتراض رسائل البريد الإلكتروني التي تحوي إشعارات لمكالمات جماعية كان يتم إجراؤها بين مكتب التحقيقات الفدرالي وقسم شرطة سكوتلاند يارد وغيرها من أقسام الشرطة العالمية. موضوع المكالمة؟ نقاش عن "التحقيقات الجارية في ما يخص جماعات أنونيمس ولولزسيك وأنتيسيك والمجموعات المتفرعة عنها". وعندما يحصلون على البريد الإلكتروني، لا يبقى على القراصنة سوى استخدام معلومات الاتصال وشيفرة الدخول المرسلة فيه ليشتركوا سراً بالمكالمة. فبينما كانت أبرز منظمات إنفاذ القانون في العالم تناقش قضية العمل ضد أنونيمس ولولزسيك، كان القراصنة جالسين يستمعون إلى الشرطة التي كانت توجز لهم، دون علمها، حالة التحقيقات الجارية. حتى إن المكالمة قد تم تسجيلها من قبل لولزسيك التاي قامت بوضعها على يوتيوب مسببة حرجاً كبيراً للسلطات التي كانت طرفاً في المكالمة.

من الأفضل إذاً عدم امتلاك حساب على الإنترنت، أليس كذلك؟

ليس بالضرورة، فصحيح أنه نظراً إلى المخاطر الناجمة عن وضع البيانات الاجتماعية على الإنترنت، قد يبدو عدم الاشتراك في الفايسبوك أو لينكدإن هو الحل الأمثل. لكن مقاطعة مواقع التواصل الاجتماعي تفرض تحديات جديدة. فحين لا تمتلك حضورك الخاص على الإنترنت ولا تسيطر عليه، من السهل جداً بالنسبة للمجرم أن يجمع المعلومات العامة المكشوفة عنك وينشئ حساباً على مواقع الوسائط الاجتماعية يستخدمه لنشاطات إجرامية متعددة، بدءاً من سرقة الهوية ووصولاً إلى التجسس. وثمة في الحقيقة العديد من الأمثلة على ذلك، خاصة لحسابات المشاهير. ففي أواخر عام 2010 على سبيل المثال، سرقت عصابة جريمة منظمة هوية الأمين العام للإنتربول، رون نوبل، وأنشأت صفحة له على الفايسبوك. وقد

حصل المجرمون على صورته الرسمية من موقع الإنتربول على الإنترنت، وانتزعوا البيانات من سيرته الذاتية الرسمية لينشئوا حساباً مزيفاً له على الفايسبوك. وبدأت العصابة بإقامة الصداقات مع كبار موظفي السلطة التنفيذية في أنحاء العالم منتحلين شخصية نوبل، وراحت تطرح عليهم أسئلة عملياتية بواسطة موقع التواصل الاجتماعي. وكان المجرمون المنتحلون لشخصية نوبل يحاولون جمع معلومات استخبارية حول عملية إنفراريد (تحت الحمراء)، وهي عملية عالمية سرية للإنتربول لتحديد موقع الفارين الدوليين ذوي الأولوية العالية واعتقالهم. ولم يتم توضيح عدد الأشخاص الذين انطلت عليهم الحيلة ولا كمية البيانات التي تم مشاركتها بالفعل، لكن الكثيرين من كبار موظفي الشرطة قبلوا طلبات الصداقة المزعومة.

الجاسوس الذي أعجب بي

وجد التجسس الصناعي أيضاً حليفاً له في الشبكات الاجتماعية. وقد سردنا في الفصل الأول من هذا الكتاب قصة شركة إيي.إم.إس.سي للتوربينات الهوائية في ماساتشوستس، التي خسرت ما يعادل مليار دولار من عوائدها بعد أن تعرضت شيفرتها الحاسوبية المصدرية للسرقة خلال عملية تجسس صينية. لكن ما لم نشرحه في ذلك الفصل هو كيف نُفذّت العملية.

عندما قرر المسؤولون الصينيون سرقة الشفيرة المصدرية لمصلحة سينوفيل، وهي شركة تابعة للدولة، كانت إيي.إم.إس.سي قد زودتها بتوربينات هوائية، فإن فحصاً بسيطاً لموقع لينكدإن زود عملاءهم بإمكانية الدخول إلى لائحة الموظفين العاملين في شركة ماساتشوستس. وحالما أنهى الصينيون مراجعة جميع الموظفين ومواقعهم في الشركة، تم وضع قائمة تُبرز الأهداف التي يمكن أن تكون أفضل المداخل إلى الشيفرة المصدرية الثمينة

لشركة إيي.إم.إس.سي. وكان أحد الأشخاص الذين تم اختيارهم هو مهندس صربي يدعى ديجان كاراباسيفتش يعمل في مكتب الشركة في النمسا.

بدأ الصينيون مراقبة كاراباسيفتش عبر مواقع التواصل الاجتماعي المختلفة، مثل لينكدإن وفايسبوك وتويتر. فعلموا أنه كان ماضياً في طلاق كريه وأن مرتبته في الشركة قد خُفضت مؤخراً، وهذه هي بالذات نقاط الضعف التي تعتبرها أية وكالة استخبارية معاصرة تبحث عن مجنّدين محتملين. ومن خلال كتاباته المتعددة على مواقع التواصل الاجتماعي، كان الصينيون قادرين على إعادة إنتاج "نموذج حياة" كاراباسيفتش، واضعين على الخريطة المقاهي والصالات الرياضية والمطاعم المفضلة لديه، ومحددين موقع منزله ومكتبه ومواعيد سفره وغيرها من الأمور الروتينية في حياته اليومية. كما علموا أيضاً أنه يميل إلى الآسيويات. مسلحين بكافة هذه المعلومات، بدأ الصينيون عملية التجنيد.

تقرب تجار صينيون من كاراباسيفتش وعرضوا عليه فرصة عمل لديهم كاستشاري. وفي النهاية، تمكنوا من إقناع كاراباسيفتش بتزويدهم بالشيفرة المصدرية (الوصفة السرية) التي سمحت لسينوفل بصناعة المحركات الهوائية الخاصة بها دون الحاجة إلى شركة إيي.إم.إس.سي. وكان كل ما يهم كاراباسيفتش هو أن التجار الصينيين أسسوا مكتباً له في بكين ووعدوه "بكل التواصل الذي يرغب به... خاصة مع زميلاته في العمل". وبعد أن تمت السرقة، تم الكشف عن مئات المحادثات على السكايب ورسائل البريد الإلكتروني بينه وبين التجار الصينيين، حيث كتب كاراباسيفتش في إحدى الرسائل: "جميع الفتيات يردن المال، وأنا بحاجة إلى الفتيات، وشركة سينوفيل بحاجة إليّ". ولكي يخففوا من مخاوفه المالية ويلبوا متطلبات مصاحبيه ويدعموا الأهداف المالية لسينوفل، قدم الصينيون لكاراباسيفتش 1 مليون دولار مقابل الحصول على الشيفرة المصدرية. وكانت الصفقة درساً

مبهراً في الاقتصاد: تلقى كاراباسيفتش 1.7 مليون دولار وخسرت شركة إيي.إم.إس.سي مليار دولار وملكية فكرية، كلها انتهت إلى شركة سينوفيل عبر بيع منتجات إيي.إم.إس.سي المقرصنة في أنحاء العالم. إنه عائد كبير على رأس المال بالنسبة لشركة سينوفل ولكل الذين لا يقفون عند الآثار الأخلاقية لمثل هذه الصفقات.

بات واضحاً الآن أن هنالك العديد من المخاطر الناجمة عن النمو الأسّي لبحر البيانات الذي نجد أنفسنا في عبابه. نحن لسنا أمام هجمة تنقيب في المعلومات تقوم بها شركات الإنترنت والمسوقون وسماسرة البيانات الآخرون وحسب، فالمجرمون والإرهابيون والحكومات المارقة، جميعهم يخضعنا إلى بطشه ومراقبته الدائمة عبر جمع البيانات ومراكمتها إلى الأبد. ولا تنفك هذه الذيول من فتات البيانات التي نخلفها وراءنا يزداد طولها زيادة أسّية بفضل الحواسب التي نحملها معنا أينما نذهب، أي هواتفنا النقالة.

الفصل السابع
هواتف تقانة المعلومات

الهواتف النقالة هي من أقل الأجهزة أمناً على الإطلاق، لذا من السهل تتبعها والتنصت عليها.

إيفجيني موروزوف

في 21 آذار عام 2012 اتصلت ميلي دولر، وهي فتاة تبلغ من العمر ثلاثة عشر عاماً من مدينة سوري في إنكلترا، بوالدها لتخبره أنها على وشك الوصول إلى المنزل. بعد ساعاتٍ، لم تصل الفتاة، ولم ترد على أي من الاتصالات على هاتفها الخلوي. ومع حلول المساء التالي، كان بحث واسع عنها قد بدأ في تلك المنطقة، وصار خبر اختفاء ميلي يتصدّر الأخبار الوطنية.

أثناء التحقيق، دخلت شرطة سوري إلى البريد الصوتي لهاتف الفتاة المفقودة أملاً بالعثور على أدلة. وكشفت المراجعات المستمرة مع شركة هاتفها النقال، أنه بعد خمسة أيام من اختفائها تم الدخول إلى نظام البريد الصوتي، وأن الرسالة الجديدة التي كانت قد وصلت ذلك المساء قد تم الاستماع إليها من قبل أشخاص مجهولين. وأعطى هذا الاكتشاف أملاً لعائلة دولر بإمكانية أن تكون ابنتهم لا تزال على قيد الحياة. ومع مرور الأسابيع، استمرت الرسائل المتروكة على بريد ميلي الصوتي بالظهور ومن ثم الحذف، ما جعل المحققين يتساءلون في ما إذا كانت الفتاة في الحقيقة هاربة.

لسوء حظ عائلة دولر، فإن ميلي لم تكن هاربة بل مخطوفة، وقد تم العثور على جثتها على بعد خمسة وعشرين ميلاً من المكان الذي شوهدت فيه حية لآخر مرة قبل ستة أشهر. في لحظة واحدة، أُعلن أن قضية ميلي هي من قضية شخصٍ مفقود إلى تحقيق في جريمة قتل. لكن حقيقة واحدة بقيت تحير الشرطة: من كان يدخل باستمرار إلى هاتف الفتاة بعد أن

فُقدت وأصبح من المسلم به أنها قد ماتت؟ هل كان ذلك الشخص هو القاتل؟ أم صديقاً غيوراً؟ أم والديها؟ بقي هذا السؤال المحير دون إجابة لما يقرب من العقد من الزمن حتى عام 2011، عندما تم حل اللغز. كان المجرم شخصاً لا يمكن لأحد أن يتوقعه أبداً.

في مقالةٍ طويلة نشرتها صحيفة الغارديان، كُشف أن هاتف ميلي كان من بين الهواتف المستهدفة من قبل أخبار العالم التابعة لروبرت مردوخ، في فضيحةٍ لُقّبت باسم هاكغيت من قبل الصحافة البريطانية. لم يتم اختراق هاتف ميلي وقرصنته من قبل قاتلٍ أو من قبل والديها أو صديقها، بل من قبل أولئك الباحثين عن سبقٍ صحافي لصفحاتهم الشعبية. ولم تكن ميلي المسكينة وعائلتها هم الضحايا الوحيدين لهاكغيت، فكذلك كان العديد من المشاهير والسياسيين وحتى أفراد من العائلة الملكية البريطانية، وهو أمر منطقي نظراً لأهميتهم كشخصيات عامة. وفي النهاية، تبين أن الصحافيين والمحققين الخاصين الذي يعملون لمصلحة أخبار العالم، وسّعوا عمليات سرقة بيانات الهواتف النقالة لتتجاوز حسابات الشخصيات العامة. حيث قاموا أيضاً بلا حياء بقرصنة الهواتف النقالة لأقارب الجنود البريطانيين الذي قُتلوا في العراق وأفغانستان، وكذلك ضحايا التفجيرات الإرهابية المأساوية التي ضربت لندن في السابع من تموز. وأدت التفاصيل المرعبة للقضية إلى حالة احتجاج شعبية شاملة، أدت بدورها إلى إغلاق صحيفة مردوخ، أخبار العالم، بعد 168 عاماً من الصدور المتواصل. وتم اعتقال العديد من موظفي ومقاولي الصحيفة، من ضمنهم المحقق الخاص الذي عُيِّن للحصول على تفاصيل عن اختفاء الفتاة الشابة.

أما الوالدان المكلومان فلم تشعرهم الاعتقالات والعقوبات التي طالت مرتكبي الجريمة براحة كبيرة بالطبع. فبالنسبة لعائلة دولر، كانت الأخبار التي تحدثت عن أن صحيفةً هي التي قامت باختراق نظام حماية هاتف

ميلي غير مفهومة أبداً. فهل أسهم هذا الاختراق غير القانوني لهاتف فتاة ضائعة عمرها ثلاثة عشر عاماً في إعاقة التحقيق الساعي إلى تحديد مكان ابنتهم الضائعة؟ أية موارد ضاعت على الشرطة وهي تحاول الوصول إلى كنه ما بدا دليلاً قاطعاً تركه قاتل ميلي المشبوه، وقت ثمين كان كافياً لمنع مأساتها وموتها الذي حل قبل أوانه. لن نعرف أبداً، وكذلك عائلة دولر، التي ستعيش مع هذه المأساة ومع هذا السؤال الحارق في كل يوم بقي من حياتها.

مع أن مثل هذه الأفعال محزنة حقاً، فإن ارتكابها في غاية السهولة. فنظام حماية هواتفنا النقالة، الأجهزة التي يحرص المواطنون العصريون على حملها على الدوام، هو مهزلة، ومن السهل استغلاله من قبل الجريمة المنظمة والمطاردين والإرهابيين، بل حتى من الصحافيين الذين يعوزهم الوازع الأخلاقي أو ذرة من الحياء.

انعدام الأمن في نظام تشغيل الهواتف النقالة

تتحول هواتفنا النقالة تدريجاً إلى حواسبنا المفضّلة. وتؤدي هذه الأجهزة الواشية الموجودة في جيوبنا دور الأدلة اللاسلكية، التي تفضح نشاطاتنا ومواقعنا. وتماماً كما تقدم الهواتف النقالة بيانات ثمينة للمعلنين، كذلك تفعل بالنسبة للمجرمين. والأسوأ من ذلك هو أن الهواتف النقالة قد تكون أقل الأجهزة أماناً على الإطلاق. فبرمجياتها معروفة بسهولة تخزينها، ومخاطرها ليست معروفة، وأنظمة حمايتها عامةً متخلفة. ونتيجة لهذا كله، فإن الهواتف الذكية من أسهل الأجهزة قرصنةً. وفيما كانت السلطات التنفيذية والخدمات الأمنية قادرة على تتبع الهواتف النقالة منذ سنوات، أصبحت التقنيات نفسها اليوم متاحة للشركات الإجرامية والقراصنة اليوميين أيضاً.

في زمننا هذا، هناك برمجيات خبيثة وأحصنة طروادة مصممة خصيصاً

لتعطي المهاجمين إمكانية الدخول إلى ميكروفون جهازك الخلوي تسجل أي صوتٍ في الجوار، حتى حين لا تكون في مكالمة. أي شيء تفعله وأية بيانات تخزنها على هاتفك النقال، تاريخ رسائلك النصيّة برمته وسجل العناوين والصور، وسجل المكالمات وكلمات سر حساباتك على الشبكات الاجتماعية ومعلومات تلك الحسابات، يمكن لكل ذلك أن يتم اعتراضه واختراقه وتقديمه للمنظمات الإجرامية للاستفادة منه في المستقبل.

يمكن استخدام البرمجيات الخبيثة على الهواتف النقالة لتتبع موقعك تتبعاً دائماً، والسماح للمجرمين برؤية موقعك بالزمن الحقيقي وعرضه على خرائط غوغل ماب على نحو مريح. بل يمكن تشغيل كاميرا الفيديو على هاتفك الذكي أيضاً (دون أي ضوءٍ منبه) ليتم تسجيل فيديو لك. هنالك العديد من الفيديوهات على يوتيوب، وكذلك مواقع تعليمية وبرامج إجرامية صنعت مقدماً للبيع، كفيلة بتمكين حتى المبتدئين من اختراق الهاتف النقال. بل إن الأمر لا يحتاج أكثر من إرسال رسالة نصية قصيرة مصابة إلى هاتف هدفك.

يحق للمرء أن يتساءل، كيف يمكن للهواتف النقالة أن تكون عرضة للاختراق بهذه السهولة؟ يكمن الجواب في نظام التشغيل. فأنظمة تشغيل الهواتف النقالة أحدث من نظيرتها العاملة على المنصات الثابتة العريقة، ولكنها أقل أمناً. يدرك المجرمون تماماً أن عالم البيانات الكبيرة ينتقل إلى الهواتف النقالة، لذا فإنهم يركزون جهودهم عليها لتحقيق أكبر العائدات على استثماراتهم في البرمجيات الخبيثة. الهاتف النقال هو منصتهم المفضلة، إذ تربطنا به علاقة حميمة وهو بصحبتنا دائماً، والمجرمون يتكيفون ويبدعون بلا هوادة.

في بدايات عام 2014، حددت مكافي حوالى أربعة ملايين نوع مختلق من البرمجيات الخبيثة للهواتف النقالة، بزيادة تقدر بـ 614 بالمئة مقارنة

بالسنة التي سبقتها. وعلاوةً على ذلك، وفقاً لدراسةٍ صادرة عن سيسكو (وغالباً ما يذكرها في محاضراته نائب الرئيس السابق الكبير لشركة أبل لشؤون التسويق العالمي، فيل سكيلير)، فإن 99 بالمئة من البرمجيات الخبيثة للهواتف النقالة موجهة ضد نظام أندرويد من غوغل. والنتائج مقلقة للغاية، خاصة إذا ما أخذنا في اعتبارنا أن 85 بالمئة من الهواتف الذكية، التي كانت تباع حول العالم، وفق إحصاءات تعود إلى منتصف عام 2014، هي أجهزة أندرويد، وأنه من المتوقع بيع مليار جهاز أندرويد إضافي بحلول عام 2017. تمثل طبيعة المصدر المنفتحة لنظام أندرويد بلا شك أحد أبرز عوامل رواجه، ولكن مع مثل هذا الانفتاح والقدرة على تخصيص البرنامج المجاني وفق الرغبة يبرز العائق الأكبر، أي الحماية. فأغلبية مصنعي الأجهزة ومزودي الخدمات الخلوية يقدمون تحقيقاً رديئاً لهذه البرمجيات.

ما الذي يجعل سرقة البيانات من أجهزة أندرويد أمراً سهلاً إذاً؟ ببساطة، إنه غياب تحديثات نظام تشغيل أجهزة الهاتف النقال وإصلاحاته. تنبثق نسخٌ جديدة لأندرويد لتصل إلى المستخدمين عبر الشركات المشغّلة كوسيلةٍ لفرض التحديثات. بالإضافة إلى ذلك، تحتاج الشركات المشغّلة وتلك المصنّعة للملحقات إلى تعديل كل إصدار أندرويد جديد، وتكييفه للعمل مع كل نموذج من الهواتف النقالة، وهي عملية مكلفة تتطلب وقتاً طويلاً، ما يؤدي في النهاية إلى حصول كل جهاز في عالم أندرويد على تحديثات قليلة. الأسوأ من ذلك، كما تبين دراسات عديدة، تسبب عمليات التخصيص وإضافة برامج غير آمنة من قبل شركات الهواتف النقالة بـ 60 بالمئة من التهديدات الأمنية في عالم أندرويد. جميع تلك التطبيقات والرسوميات المزعجة التي تأتي مع هاتفك، والتي تعرف باسم البرامج البدينة لأنها تأخذ مساحة كبيرة على الجهاز، مشكوك في قيمتها وهي لا تعدو أن تكون وسائل للتحايل بغرض التسويق للشركة المصنعة ولمزود الخدمة اللاسلكية. وهي

ليست مزعجة فقط، بل إن رداءة تحقيقها تقود إلى أغلبية التهديدات الأمنية على أجهزة أندرويد.

بالمقارنة، تتحكم شركة أبل بكافة بيئات أجهزتها البرمجية والعتادية. ما يسمح لها بضمان عمل نظام تشغيل هاتف آيفون (آي.أو.إس) بسلاسةٍ أكبر، وتمنع شركات التشغيل من تعديل نظام التشغيل الضمني بإضافة برامجها البدينة. إن المقارنة بين أندرويد ونظام تشغيل الآيفون تخبرنا القصة التالية: بعد خمسة أشهر على إطلاقه عام 2013، كانت 82 بالمئة من أجهزة أبل البالغ عددها 800 مليون، تستخدم الإصدار السابع من نظام آي.أو.إس، وهو أحدث نسخة لنظام التشغيل تطلقها شركة أبل. بالمقارنة، لا يستخدم أكثر من حوالى 4 بالمئة من أجهزة أندرويد أحدث إصدار من النظام، والذي أطلق في العام نفسه. المحبط حقاً في هذه الأرقام هو أنه لو قام جميع مستخدمي أندرويد بتنصيب كافة التحديثات من النسخة الجديدة من نظام تشغيل الهاتف النقال، لأمكن تجاوز 77 بالمئة من التهديدات القائمة. فإخفاق غوغل وشركاؤها في توفير تحديثات الحماية على نطاقٍ واسع لقاعدة المستخدمين هو الذي يمنح للمجرمين الوقت الذي يحتاجون إليه للعثور على نقاط الضعف في نظام تشغيل أندرويد، الواحدة تلو الأخرى، واستهدافها في هجماتهم.

احذر من التطبيقات

ليست الشركات المصنعة للتطبيقات مثل روفيو وزينغا وسنابشات، هي وحدها التي تنشئ التطبيقات لجمع بياناتك وبيعها، فقد دخلت عصابات الجريمة المنظمة هذا المعترك أيضاً. فقد يفترض المرء منطقياً أن أي تطبيق يضعه منتجوه على متجر تطبيقات غوغل أو أبل، تخضع شيفرته البرمجية ومطوّره إلى مراجعة أمنية دقيقة، ولكن الأمر ليس كما يبدو. فبوجود أكثر من مليون تطبيق في كل من نظامي تشغيل أندرويد وآي.أو.إس، يُجرى

القليل جداً من التحقق البشري من هذه التطبيقات، وهذه حقيقة يعرفها المجرمون، الذين دمروا متاجر التطبيقات في غير مناسبة. بدلاً من ذلك، تقوم خوارزميات الحواسب المؤتمتة بالجهد الأكبر في عملية المراجعة، بينما يأمل مطورو متجر التطبيقات أن يفي ذلك بالغرض.

نتيجة لذلك تشيع الأخطاء وتتكاثر التطبيقات التي تحتوي على البرمجيات الخبيثة، في المواقع التي من المفترض أن تكون مواقع تطبيقات حسنة السمعة. مع بداية عام 2013 كان قد اكتُشف أن أكثر من اثنين وأربعين ألفاً من التطبيقات في متجر تطبيقات غوغل، تحتوي برامج للتجسس وأحصنة طروادة تسرق المعلومات. تهاجم البرمجيات الخبيثة الموجود في هذه التطبيقات البيانات الموجودة على هاتفك، وخاصة المعلومات المالية. فبعد عدة أيام فقط على إطلاق متجر تطبيقات أندرويد، كان المجرمون قد قاموا بتحميل تطبيقات مصرفية مزيفة لكبريات المؤسسات المالية في أنحاء العالم. وكانت هذه التطبيقات واقعية جداً تستخدم شعارات البنوك وخطوطها وألوانها ورسومها الأصلية لتدعم صدقيتها. ووقع عشرات الآلاف من الناس بالشرك بتنزيل هذه التطبيقات، وعندما كانت تفشل في عملها، كان الزبائن الغاضبون يتصلون بالبنوك ليكتشفوا أنه "ليس لدينا تطبيق أندرويد حتى الآن".

عدل المجرمون السايبريون عملياتهم بتطوير المزيد من التطبيقات المصرفية المزيفة. ومع أنه تم تحديد ما لا يزيد عن سبعة وستين حصان طروادة مصرفياً عام 2012، إلا أن الرقم ازداد ليصل إلى أكثر من ألف وثلاثمئة في نهاية عام 2013 وفقاً لمختبر كاسبرسكاي. وقد تم حتى الآن اكتشاف مجموعات من برمجيات خبيثة الهواتف تستهدف زبائن أضخم البنوك في العالم، مثل سيتي بانك وآي.إن.جي والبنك الألماني إتش.إس.بي.سي وباركليز، وست وستين مؤسسة مالية أخرى حول العالم.

تزداد هذه البرمجيات الخبيثة غزارة في مواقع الأطراف الثالثة. ففيما توجد رقابة أمنية خوارزمية محدودة على الأقل في سوق أندرويد الرسمي، غالباً ما تغيب مثل هذه الرقابة تماماً في مواقع الأطراف الثالثة. نتيجة لذلك، وُجد أن أكثر من خمسمئة بائع للتطبيقات من تلك الأطراف الخارجية، يعرضون تطبيقات لأندرويد تحتوي على برمجيات خبيثة. وبسبب غياب المراجعة الأمنية في مواقع التطبيقات هذه، فإن التطبيقات التي تَحمل فيروسات وأحصنة طروادة يمكن أن تستمر في العمل مدى الحياة لتقدم دخولاً سنوياً للمجرمين الذين ينشئونها ويحملونها على المواقع.

ربما كان هذا أكثر ندرة بكثير، إلا أنه تم العثور على تطبيقات خبيثة في متجر تطبيقات أبل أيضاً. بالرغم من أن نظام تشغيل آيفون منظم ومضبوط بشكل أكبر، إلا أن العديد من المستخدمين يجدون هذه البيئة خانقة. فعندما يشترون منتجاتهم في البداية، لا يمكن لمستخدمي آيفون ضبط لوحات المفاتيح أو تغيير محرك البحث أو إدارة الملفات محلياً، أو إضافة الأدوات إلى النوافذ الرئيسية، وهي كلها ميزات قياسية في نظام أندرويد. ولتجاوز هذه القيود، يقوم العديد من مستخدمي هذه الهواتف "بإطلاق سراح" هواتفهم، مستخدمين برنامجاً متخصصاً يمكنهم من اختراق هواتفهم بنفسهم لكي يحصلوا على سماحيات إدارية على هواتفهما تمكنهم من التحكم بالميزات المحجوبة من قبل شركة أبل. يسمح تحرير جهاز يعمل بنظام آي.أو.إس للمستخدمين بالحصول على آلاف البرامج التي لا تسمح بها شركة أبل رسمياً. وقد تم تحرير عشرة ملايين جهاز تقريباً، ما مكن مستخدميها من الاستفادة من متاجر تطبيقات تابعة لأطراف ثالثة، مثل موقع سيديا، لتحميل تطبيقاتهم. وفيما يمنح تحرير هذه الأجهزة المستخدمين تحكماً أكبر بهواتفهم، فإنه يفتح أجهزة آي.أو.إس هذه على

التهديدات الأمنية نفسها الشائعة في أنظمة أندرويد، بما فيها التعرض لمختلف أنواع الاحتيال المالي.

لماذا يحتاج تطبيق المصباح للدخول إلى جهات الاتصال لدي؟

قام مئات الملايين من مستخدمي الهواتف الذكية حول العالم بتنزيل تطبيق المصباح الضوئي الشائع والمريح. وهو مفيد جداً عندما نبحث عن مفاتيحنا في محفظتنا أو عندما نحاول فتح الباب في وقت متأخر من الليل، ومعظمنا لم يدفع شيئاً على الإطلاق مقابل هذا الامتياز. لكن لماذا يحتاج هذا التطبيق إلى الدخول إلى جهات الاتصال لديك؟ ولماذا يسأل عن مكانك؟ ينبغي أن يكون مكاني واضحاً: أنا في الظلام؛ ولذلك أحتاج إلى تطبيق المصباح! لكن سرعان ما يتضح أن معظم هذه التطبيقات، وخاصة في نظام أندرويد، ليست سوى آليات مريحة لسرقة بياناتك وتنزيل كافة جهات الاتصال لديك والتحقق من موقعك باستمرار، ووضع برامج تسجيل نقرات لوحة المفاتيح، وجمع معلوماتك المالية. والنتيجة هي ما نشهده من تحويل للجريمة إلى تطبيقات واختزال الأعمال الإجرامية إلى مجرد تطبيق للهاتف النقال على بساطته.

السماحيات الممنوحة لهذه التطبيقات، وخاصة في بيئة أندرويد، حيث لا مجال لحجب سماحيات محددة لأحد التطبيقات قبل تنصيبه، تعني أنك وبياناتك في خطر. تشبه السماحيات الممنوحة للتطبيقات على أجهزة الهاتف شروط الخدمة، فجميعنا ينقر على زر القبول دون أن يفكر حقاً بالمعاني الضمنية لهذا القرار. يعني هذا الترخيص في الواقع أن مطور التطبيق المجرم أو المحتال باتت لديه الآن السلطة التي يحتاج إليها ليقوم بالاحتيال أو السرقة من حسابك المصرفي عن طريق جهازك النقال.

يُنشئ المجرمون أيضاً تطبيقات مزيفة مخصصة للاحتيال عن بعد. فثلاثة أرباع البرمجيات الخبيثة للهواتف الخلوية تستغل نقاط الضعف الموجودة

في أنظمة الدفع للهواتف، عن طريق إرسال رسالة قصيرة احتيالية إلى أرقام غير مجانية لتعود كل رسالة بربح فوري يقدر بعشرة دولارات. فإذا ضربنا المبلغ بمئات الآلاف من الرسائل، يصبح المبلغ هائلاً. حدث ذات مرة أن تمكن المحتالون من وضع نسخ مزيفة من ألعابٍ مشهورة، مثل الطيور الغاضبة وأساسين غريد على متجر للتطبيقات. وحالما يتم تحميل التطبيق يبدأ، في كل مرة يشغله المستخدم، بإرسال ثلاث رسائل ذات قيمة دون علم المستخدم بتكلفة 7.50 دولاراً لكل رسالة. ولم تكن سوى ساعات حتى تمكن اللصوص من جمع عشرات الآلاف من الدولارات عن طريق الرسوم الاحتيالية.

تُستخدم الهواتف النقالة المسروقة على نحو متزايد، لإرسال رسائل إلكترونية مزعجة، عبر ضمها إلى ما يُدعى الشبكات الروبوتية. هذه الشبكات هي عبارة عن مجموعة من الحواسب المستعبدة المصابة بالبرمجيات الخبيثة، والتي تعمل بالتنسيق في ما بينها ويسيطر عليها القراصنة أو المجرمون لنشر كميات كبيرة من البريد الإلكتروني المزعج، أو للمشاركة في هجمات حجب الخدمة دون علم صاحب الجهاز الحقيقي. وكانت الشبكات الروبوتية مقتصرة على أجهزة الحاسب المكتبية أو المحمولة، أما الآن فقد تم تجنيد ملايين الهواتف النقالة في هذا الإطار، وتقع هذه الأجهزة المسيّرة تحت السيطرة التامة للمجرمين والقراصنة، الذين يضمونها إلى "شبكات الزومبي" التي يديرونها والتي تنمو نمواً أسّياً. تكمن هذه الشبكات الواسعة من الأجهزة المقرصنة منتظرة وجاهزة للانطلاق ضد أي هدف، حالما تتلقى الإشارة. بما أن مبيعات الهاتف النقال قد تجاوزت مبيعات الحواسب المكتبية والمحمولة بنسبة عشرة إلى واحد، فمن الواضح أن مستقبل الحوسبة يميل إلى الهواتف النقالة. وقد أدرك المجرمون أن مستقبل سرقة البيانات وهجمات حجب الخدمة والبرمجيات

الخبيثة يكمن أيضاً في الهواتف النقالة.

حتى التطبيقات القانونية يمكن أن تعرضك وبياناتك للخطر إذا كانت برمجتها رديئة، أو إذا احتوت على نقاط ضعف أمنية غير معروفة. كما كانت الحالة مع التطبيق المشهور "حجرة الصورة الاجتماعية" أو المعروف باسم سنابشات. فسنابشات هو خدمة تسمح للمستخدمين بإرسال صور شخصية (سيلفي) (غالباً ما تكون عارية) لتختفي، على حد زعمهم، خلال بضع ثوانٍ على وصولها إلى هاتف المتلقي. وقد تم إرسال أكثر من مليار صورة بواسطة هذه الخدمة، وفي أواخر عام 2013 حاول فايسبوك شراء الشركة مقابل 3 مليارات دولار لكنه فشل في ذلك. وفي بداية عام 2014 اتضح أن سنابشات كان يحتوي على خلل أمني عرّض الملايين من مستخدمي آيفون لهجمات حجب الخدمة.

كانت نقطة الضعف تسمح للقراصنة باستهداف هاتفك بالتحديد، عن طريق إرسال آلاف الرسائل من نمط سنابشات في غضون خمس ثوانٍ فقط، بما يكفل تعطيل هاتفك وجعله غير قابل للاستخدام، إلى أن تقوم بعملية إعادة إقلاع إجباري للجهاز. علاوةً على ذلك، تمكن القراصنة أيضاً من اختراق حوالى خمسة ملايين حساب لمستخدمي سنابشات، ونشروا على مواقع القراصنة الخاصة بهم قاعدة بيانات تحتوي أسماء هؤلاء المستخدمين وأرقام هواتفهم. والأسوأ من ذلك، كما كشف في ما بعد، هو أن الميزة الرئيسية لسنابشات، وهي القدرة على إرسال صور عارية تدمر نفسها تلقائياً بعد عشر ثوانٍ أو أقل، قد اخترقت أيضاً. فخلافاً للوعود، لم تدمر الصور نفسها وبقيت قابلة للاسترجاع في كلٍّ من هاتف المتلقي ومخدمات حواسب سنابشات. نتيجة لذلك، ظهرت على الإنترنت عشرات الآلاف من صور سنابشات التي كان يعتقد بأنها حُذفت، فوُضِعتْ على موقع إنستاغرام وعلى العديد من المواقع الإباحية الانتقامية. بعد ذلك تم

استخدام الصور لأغراض الابتزاز وغيرها من الاعتداءات الإجرامية.

الأجهزة النقالة والتهديدات الشبكية

لا تؤثر التهديدات الناشئة للبيانات التي نحملها على هواتفنا على المستهلكين، بل لها أثر كبير على الشركات أيضاً. ففي الشركات المعاصرة اليوم، أصبح شعار "أحضر جهازك بنفسك" هو المقياس، حيث يمنح الموظفين امتياز الدخول إلى البيانات والتطبيقات التجارية الحساسة من خلال أجهزة هواتفهم الخاصة. ويدخل حوالى 89 بالمئة من الموظفين اليوم إلى المعلومات المتعلقة بعملهم باستخدام هواتفهم، ويقوم حوالى 41 بالمئة منهم بهذا العمل دون إذنٍ من الشركات التي يعملون بها.

تعني هذه الظاهرة، التي أصبحت ممارسة قياسية في مكان العمل اليوم، أن المزيد والمزيد من المعلومات التجارية باتت في خطر، بفضل هجمات برامج التجسس ضد أجهزة الهاتف. وحتى عندما يتم إقفال شبكة الشركة وحمايتها، فإن أجهزة الهاتف الشخصية تشكل مكاناً تسهل فيه سرقة البيانات. ولن تضيع المنظمات الإجرامية وقتها باستهداف أكثر أماكن تخزين المعلومات أمناً؛ بل ستلاحق دوماً الحلقة الأضعف في السلسلة حتى تحصل على مُبتغاها.

يتنامى إبداع المجرمين في استهداف المعلومات على هاتفك، بل على شبكات الهواتف نفسها. فمقابل بضعة دولاراتٍ، يمكن للمجرمين أن يشتروا ويهيئوا محطة خلوية مصغرة، وهي توسعة للشبكة اللاسلكية تساعد الناس على تحسين خدمة الهاتف النقال في المناطق ذات الإشارة الضعيفة. هذا الجهاز هو في الواقع برج مصغر للهواتف النقالة، ويمكن للمجرمين تعديله لخداع جهازك وجعله يعتقد أنه يتصل ببرج حقيقي، بينما هو يتصل ببرج متنقل يُشغّل ويُدار من قبل المجرمين. أما هدفهم من قيامهم بذلك فهو الحصول على كافة البيانات المرسلة من هاتفك، مثل كلمة سر

حسابك المصرفي أو أية رسائل بريد إلكتروني هامّ قد ترسلها. تمتاز المحطات الخلوية المخادعة هذه بفعالية خاصة في مجال التجسس الصناعي، إذ لا يحتاج القراصنة سوى إلى تثبيت الجهاز قرب سور شركتك حتى يحصلوا على البيانات الصادرة عن أجهزة هواتف مئات الموظفين في الشركة. ومن الأهداف الرئيسية الأخرى المطارات والمؤتمرات، التي يجتمع فيها الكثير من رجال الأعمال. وسرعان ما يتضح أنك لست الوحيد الذي يجد بيانات هاتفك الذكي مشوقة.

قرصنة مدفوعات الهواتف النقالة

لا تزال أجهزة الهاتف النقال في الوقت الحالي في مراحل تطورها البدائية بالطبع، والعديد من الحساسات الحديثة، مثل معرفات التردد الراديوي (آر.إف.آي.دي) واتصالات النطاق القريب (إن.إف.سي)، ستقدم للهواتف النقالة إمكانيات جديدة، تصحبها نقاط ضعف جديدة. أحد الجوانب التي يتجلى فيها ذلك هو اختفاء العملة المادية. ستكون عملة المستقبل نقالة وافتراضية، وثمة حشد من الحساسات والتطبيقات الجديدة في طريقها لأن تحل محل محفظتك والنقود التي في جيبك. بل إن بعض مشغّلي الهواتف النقالة، مثل سفاريكوم في أفريقيا، يهيمنون على كامل نطاق التسديد. ففي كينيا على سبيل المثال، يتم إجراء المناقلات المتعلقة بـ 25 بالمئة من الناتج القومي من خلال نظام دفع إم – بيسا، التي تقدمه سفاريكوم. لقد أصبحت أنظمة التسديد المالي عن طريق الهواتف النقالة، التي لم تكن موجودة أصلاً في نهاية القرن الماضي، متوفرة الآن في أكثر من سبعين بلداً، ويتم استخدامها لتداول مليارات الدولارات شهرياً. وكانت هذه الأنظمة مفيدة على نحو خاص، في إدخال من لم يكن لديهم حساب مصرفي في العالم النامي إلى عالم التجارة، تاركة أثراً إيجابياً لا يستهان به على الاقتصادات المحلية.

كان هنالك توجه نحو تبني ونشر أنظمة الدفع، عن طريق الهواتف النقالة في العالم المتطور أيضاً. وقد نفذت شركات مثل ماستر كارد وفيزا، العديد من برامج الدفع عن طريق اتصالات النطاق القريب، الذي يسمح للمستخدمين بتشغيل تطبيق على هواتفهم والتلويح بالجهاز أمام حساس لاسلكي لتقتطع بسرعة تكاليف البضائع والخدمات. من ستاربوكس إلى بيست باي إلى عدادات مواقف السيارات في سان فرانسيسكو، وصولاً إلى سيارات الأجرة في مدينة نيويورك، تزداد شعبية تقنية الدفع بالتلويح (wave and pay) في عمليات دفع الحساب وتسديد الأموال. بالرغم من أن غوغل كان أول من تبنى أنظمة الدفع عبر اتصال النطاق القريب إن.إف.سي في أجهزة أندرويد، إلا أن شركة أبل واكبت هذا الركب في أيلول عام 2014، حين أضافت تقنية الدفع بالسحب (swipe and pay) إلى أحدث مجموعة من أجهزة الآيفون. ويسمح نظام غوغل واليت للدفع، أو محفظة غوغل، ضمن بيئة أندرويد للمستخدمين بتخزين معلومات بطاقات الائتمان والاقتراض الخاصة بهم لدى غوغل، ومن ثم تشغيل تطبيق غوغل واليت لدفع الحساب في عدد متزايد من المتاجر عن طريق أية طرفية سداد بالمرور. وتعمل محفظة غوغل مع شرائح اتصال النطاق القريب إن.إف.سي على عدد كبير من أجهزة الهاتف، مثل إتش.تي.سي وإل.جي وموتورولا وسامسونغ.

أما النقود، كما يتم تمثيلها على هذه الأجهزة النقالة، فليست سوى مجرد بيانات يتم تخزينها في تطبيقات هشة غير آمنة تحكمها أنظمة تشغيل نقالة ضعيفة للغاية، تستخدم تقنيات الحساسات وبروتوكولاتها لنقل البيانات غير الآمنة. أما النتيجة الواضحة فهي أن مستقبل أموال الهواتف النقالة هو أيضاً مستقبل النشل النقال. فقد سبق أن تعرض نظام محفظة غوغل إلى التخريب من قبل المجرمين في حوادث عديدة، وثمة تطبيقات

عديدة، مثل واليت كراكَر، تسمح لأي شخص برؤية الرقم الشخصي المحدد للهوية (PIN) التابع لهذا النظام عند الطلب. إضافة إلى ذلك، إذا أضاع شخص هاتفاً يعمل بنظام أندرويد، فإن أي مالٍ محفوظ سابقاً في غوغل واليت (على شكل بيانات على الجهاز)، يمكن إنفاقه بسهولة في أي متجر من قبل أي شخص يحدث أن يكون قد سرق الجهاز أو عثر عليه. ومع ازدياد انتشار تطبيقات اتصال النطاق القريب ودخول شركة أبل إلى أنظمة التسديد النقالة، فإننا بلا شك سنشهد ازدياداً في اهتمام القراصنة باستهداف أجهزة الاستقبال هذه وغيرها الموجودة في أجهزة الهاتف، بما فيها نظام تحديد الموقع الجغرافي جي.بي.إس.

موقعك يصبح مسرح الجريمة

ليس المعلنون وسماسرة البيانات هم وحدهم المهتمين بالتتبع المستمر لموقعك. فقد وجد المجرمون والمحتالون والمطاردون بدورهم استخداماً نافعاً لشريحة الموقع الجغرافي على هاتفك الذكي. وغالباً ما يبني القراصنة على العمل الجيد الذي قام به سماسرة البيانات مسبقاً، كوسيلة لتخريب البيانات التي قمت أنت بتسريبها. لنأخذ على سبيل المثال تطبيق تيندر للمواعدة اعتماداً على الموقع، والذي تطرقنا للحديث عنه في الفصل الرابع من هذا الكتاب. فنظراً لهذه الكميات من البيانات والصور البذيئة وأعداد الشركاء الجنسيين المحتملين، لم يكن من المفاجئ أن يبذل القراصنة ما بوسعهم للوصول إلى نقطة ضعف أمنية في التطبيق، تسمح لأي شخص باكتشاف مكان شخص آخر بالزمن الحقيقي ضمن نطاق خمس أقدام، وهي معلومة يفترض أن تبقى سرية. وأفضل سيناريو يمكن أن يحدث بفضل بيانات الموقع هذه هو تجربة غرامية إيجابية. أما أسوأ السيناريوهات فهو أن يتم استغلاله من قبل تطبيقات محتالة، على غرار تطبيق "الفتيات من حولي" الذي أثبت أنه أداة جبارة في يد المحتالين

والمغتصبين والبيدوفيليين. بل إن شرطة جنوب أستراليا نبهت الناس عام إلى أن بيدوفيليين كانوا يستخدمون بيانات سمات الموقع الموجودة في صور الأطفال الموضوعة على الإنترنت، لتحديد أهدافهم المحتملة وملاحقتها، ما يعرض من يظهر في هذه الصور إلى الخطر.

يزداد استخدام بيانات الهواتف النقالة لإحداث أثر سيئ في حالات الخلافات العائلية والعنف المنزلي. ففي عام 2012 كشفت وزارة العدل الأميركية أنه كان هنالك 3.4 ملايين ضحية للمطاردة سنوياً من بين مئات آلاف الأشخاص الذين يتم تتبعهم بواسطة برامج التجسس واختراقات نظام تحديد المواقع جي.بي.إس. إنه عالم "حدد وانقر" للمراقبة. لنوضح ذلك، فإن استخدام برنامج تجسس كهذا يُعتبر اعتراضاً غير قانوني استناداً للقانون الفدرالي وهو عمل غير شرعي، لكن الأدوات متوفرة دائماً حتى للقراصنة المبتدئين أو السابقين الذين ليس لديهم تجربة سابقة. ويمكن لأحد المنتجات، واسمه موبايل سباي، أن يحول أي هاتف إلى جهاز تسلل لتسجيل كل ما يدور في محيطه، حتّى حين لا تكون ثمة مكالمة جارية. وتقدم الشركة أيضاً منتجاً "لمراقبة آيباد"، ويحتوي برنامجه على نمط "كاميرا الاستراق" الذي يسمح لطرف ثالث بتفعيل ومراقبة الكاميرا عن بعد بالزمن الحقيقي، وتخزين أية صورة أو فيديو يختارون تسجيلها من جهازك على المخدم الرئيسي لتنزيلها في ما بعد. وهنالك منتج آخر اسمه، موبيستيلث (Mobistealth)، استُخدم في عام 2011 من قبل مجرم مُدان هو سيمون غيتاني، الصديق الغيور والبذيء، ليراقب نشاط هاتف خطيبته ليزا هارنون في سيدني بأستراليا. هكذا، وعندما أرسلت هارنون رسالة قصيرة إلى صديقتها تفضي لها فيها عن نيتها إنهاء العلاقة السيئة مع صديقها، تم إعلام غيتاني فوراً بهذه النية على هاتفه الشخصي عن طريق موبيستيلث.واتجه غيتاني، الذي غضب جداً لذلك، بسيارته نحو منزلها،

وبعد مشادة كلامية قام برميها من شرفة شقتها الكائنة في الطابق الخامس عشر.

لكن المتعسفين المنزليين في بعض الحالات لا يحتاجون حتى إلى إضافة برنامج تجسس من طرف ثالث على هواتفهم، بل يكفي أن يفعلوا برنامج فاميلي ماب، أو خريطة العائلة المقدم كخدمة من مزود الخدمة اللاسلكية إيي.تي.إند.تي، التي تسمح لصاحب حساب الهاتف الخلوي بتتبع كافة الأجهزة الموجودة في مخططه. وباستخدام هذا البرنامج، تمكّن أندريه ليتيف من سكوتسديل في أريزونا من تحديد موقع زوجته التي انفصل عنها وولديهما، الذين قتلهم في ما بعد. لم يعد ضرورياً اليوم أن تدفع مقابل مثل هذه الخدمة من شركات مثل AT&T، فقد باتت هذه الميزات موجودة مسبقاً في كل من نظام آيفون ونظام أندرويد. إذ يمكن تفعيل خدمات مثل "أوجد أصدقائي" (Find My Friends) و"أوجد هاتفي" (Find My Phone)، لملاحقة الآخرين عن بعد. للمساعدة على التغلب على هذه التهديدات، تعلمت مآوي الحماية من العنف المنزلي أن تتخلص من الهاتف النقال لأي ضحية جديدة، بمجرد وصولها إلى مقارّها بإزالة البطارية وتدميرها لكي لا تصبح مرشداً لاسلكياً للمطاردين والمتعسفين. ليس ضحايا العنف المنزلي الوحيدين الذين عليهم توخي الحذر من مشاركة مواقعهم دون قصد، فلدى الجنود في ساحة المعركة أسبابهم التي تدعو للقلق مع مراقبة الإرهابيين لنشاطاتهم على الإنترنت انتظاراً لفرصة مناسبة للهجوم.

"هل تستحق شارة تنالها على موقع فورسكوير أو تسجيل الدخول المجازفة بحياتك؟". كثيراً ما يطرح الجيش الأميركي هذا السؤال اليوم على جنوده، وهو ليس مجرد خطابة إذا كان الإرهابيون يستغلون البيانات الموسومة بموقع جغرافي. فعندما تلقت القوات العسكرية الأميركية

الأسطول الجديد من طائرات الأباتشي العمودية AH-64 في قاعدتها في العراق على سبيل المثال، قام بعض المجندين بوضع صور لهم على الفايسبوك وهم أمام طائراتهم الجديدة. ومن دون علمهم، قامت هواتفهم بتضمين إحداثيات مواقعهم في الصور. ولم يكن المتمردون يراقبون حسابات الجنود على الفايسبوك وحسب، بل كانوا أيضاً يقومون بتنزيل الصور وتحليلها بحثاً عن معلومات استخبارية مفيدة. وقد سمحت معلومات خطوط الطول والعرض الموجودة في الصور للإرهابيين بشن سلسلة محكمة من الهجمات بقذائف الهاون، أصابت مباشرة أربعاً من طائرات الأباتشي التي كانت قد وصلت لتوها إلى المجمع.

لا يقتصر الأمر على تتبعنا عن طريق البيانات التي نسربها من هواتفنا النقالة والملفات المدمجة، مثل الصور والفيديوهات، فنحن نقوم على نحوٍ متزايد بتسريب البيانات المرتبطة بمواقعنا في العالم المادي. وأجهزة تحديد المواقع التجسسية رخيصة الثمن يمكن شراؤها عن طريق الإنترنت، بل متوفرة للبيع في مجلة سكايمول التي نجدها أمامنا في كل رحلة طيران نقوم بها. في ذلك الدليل، يبيع تراكينغ كي جهاز تحديد الموقع الجغرافي الذي يتم تثبته إلى أية سيارة بواسطة مغناطيس أو مشبك فيلكرو، ويسمح لصاحب الجهاز باستعادة كل مكان ذهبت إليه السيارة عن طريق خريطة موجودة على الإنترنت، محدداً سرعة السيارة في كل ثانية. هذا الجهاز مفيد في معرفة "ما إذا كان مراهق يقود مسرعاً أو أين تذهب زوجتك أو زوجك أو أين يتجول موظفوك". لم تكن مثل هذه التقنيات الحديثة توجد في السابق سوى لدى وكالة تجسس أو في مكتب التحقيقات الفدرالي. أما الآن، ومع الهبوط النسبي في أسعار هذه التقنيات، يمكن لأم في الجوار أن تتجسس على أولادها أو على زوجها الذي ربما كان يخونها.

في عالم البيانات الكبيرة، قد نسرب موقعنا المادي دون الحاجة إلى

التنصت على هواتفنا أو تتبع سيارتنا بأجهزة جي.بي.إس مخفية فيها. فالتقنية الجديدة والمعروفة باسم القارئ الآلي للوحة السيارة أو إيي.إل.بي.آر، تسمح لكل من الحكومات والأفراد باستخدام كاميرات الفيديو وتقنيات التعرف البصري، لتسجيل مواقع السيارات حين انتقالها من نقطة مراقبة إلى أخرى، لتكشف تحركات أي مركبة بالزمن الحقيقي في أنحاء المدينة أو البلد بأدق التفاصيل. من مينيسوتا إلى نيوجيرسي، ومن أنقرة إلى سيدني، يتم تخزين مئات ملايين التسجيلات المستقلة للوحات السيارات. وهكذا يمكن توجيه استفسار إلى قواعد البيانات الضخمة هذه لتحديد مكان أية سيارة وفي أي وقت. والمثير في الأمر هو أن تلك السيارات التي يتم تصويرها غالباً ما لا تكون موضع اتهام أو شك في جريمة ما، لكن هذه البيانات يتم تخزينها على كل حال، لأنه يمكن الاستفادة منها في التحقيقات الجنائية في وقت ما في المستقبل.

ثمة وحدات قراءة لوحات السيارات يتم تركيبها في سيارات الشرطة أيضاً، بل وحتى في سيارات القطر، ما يوسع قواعد البيانات تلك إلى حد كبير. كما تقوم شركات خاصة مثل شركة Digital Recognition Network في تكساس وشركة إم.في.تراك في إلينويس ببناء قواعد بيانات إيي.إل.بي.آر ضخمة، لتبيعها إلى عملاء يعملون في مجال استرداد السيارات. وهكذا، إذا تأخر شخص ما عن دفع مستحقاته المالية، يمكن لهذه الشركات تحديد المواقع التي زارتها السيارة ومن ثم إرسال سيارة القطر لاستعادتها. تماماً كما تجوب سيارات غوغل ستريت فيو شوارع مدينة لتسجل فيديوهات لكل ما تراه، كذلك تفعل شركات قارئات لوحات السيارات الخاصة. فهي تلاحق سيارتك وتحدد موقعها أمام بيتك أو في عملك وفي كافة الأماكن التي تذهب إليها للتسوق. ويستفاد من هذه البيانات مالياً في ممارسة كانت عام 2014 قانونيةً تماماً. لكن مع تكاثر

قواعد البيانات هذه وانتشاراها ستنمو أيضاً المخاطر المتعلقة بالخصوصية والجريمة.

إن كانت شركتا إكسبيريان وأكسيوم عرضة لتسرب البيانات أو بيعها إلى المنظمات الإجرامية، فبمَ يختلف عنها باعة بيانات قارئات لوحات السيارات؟ أي إنه حتى ضحايا العنف المنزلي الذين ليس لهم حضور على الإنترنت أو لا يحملون هاتفاً نقالاً معهم قد يظلون عرضة للمطاردة عن طريق الأماكن التي يذهبون إليها بسياراتهم. لقد سبق لنا أن تعرفنا عمليات إساءة استعمال لبيانات قارئات لوحات السيارات في الماضي منذ عام 1998، عندما قام ملازم في شرطة مقاطعة كولومبيا في واشنطن باستخدام نظام حاسوبه لتحديد أصحاب السيارات التي كانت واقفة في موقف أشهر ملهى لغير الأسوياء جنسياً في المدينة، واستخدم البيانات في ما بعد لابتزاز الرجال، مهدداً بفضحهم إذا لم يدفعوا له رشوة. بينما قد تختلف طبيعة التهديدات المتعلقة ببيانات قارئات لوحات السيارات في وقتنا الحاضر، فإنها لا تزال موجودة من دون شك. فكيف يمكن استخدام هذه البيانات في قضايا الطلاق (كانت سيارة الزوج واقفة أمام بيت امرأة أخرى) أو من قبل شركات التأمين على الصحة (إننا نرى سيارته تقف أمام الملهى خمسة أيام في الأسبوع)؟ بل ثمة بعد مخاطر أخرى، فأنظمة قراءة لوحات السيارات ليست معصومة عن الخطأ في قراءتها لبيانات اللوحة المعدنية، والأخطاء قد تقود إلى عواقب خطرة. في عام 2009، أُوقفت سيارة امرأة تبلغ من العمر سبعة وأربعين عاماً على جانب الطريق في سان فرانسيسكو من قبل عدة سيارات شرطة في نقطة تفتيش، وصوب ستة عناصر أسلحتهم باتجاهها، وكل ذلك لأن نظام قراءة اللوحات أخطأ في قراءة أحد أرقام اللوحة المعدنية لسيارتها واعتبر أن هذه السيارة مسروقة، بينما لم تكن في الحقيقة سوى لسيدة متوجهة لشراء البقالة.

حتّى باعة التجزئة بدؤوا بسرقة تفاصيل مواقعنا بطرق جديدة وغير متوقعة. فعلى سبيل المثال، بدأ مجمع نوردستورم بتتبع زبائنه، عن طريق إشارات شبكتهم اللاسلكية وعناوين الماك الخاصة بأجهزتهم الذكية عندما يقومون بالتسوق في متاجره. فبينما تتنقل بين المحالّ، يقوم نوردستورم بملاحقتك رقمياً ليرى كم من الوقت أمضيت في شراء الملابس الداخلية النسائية مقابل شراء الأحذية الرجالية. وكان المجمع التجاري المتطور متعاقداً مع بيوكليد، وهي شركة مختصة بمساعدة الباعة على تتبع تحركات الزبون بواسطة الاتصالات اللاسلكية داخل المخزن. وقد قامت بيوكليد حتى تاريخها بتتبع وتسجيل بصمات أكثر من خمسين مليون جهاز هاتف في أربعة آلاف موقع مختلف عبر خدمتها، من بينها المئات من متاجر التجزئة الوطنية مثل هوم ديبوت. أجل، الشركة نفسها التي سربت ستة وخمسين مليون بطاقة ائتمانية بعد اختراق للبيانات في أيلول عام 2014، تريد اليوم جمع المزيد من البيانات عنك وعن موقعك ضمن متاجرها. بغياب أية ضوابط تنظم هذه الظاهرة، لا شك في أن التسوق تحت المراقبة سيصبح المعيار السائد الجديد، وأن التكنولوجيا ستتحول بشكلٍ متزايد إلى ملاحقة الناس في الفضاء المادي خارج نطاق الإنترنت.

في نوردستورم، الإشعار الوحيد الذي أعطي للزبائن عن استخدام تقنية التتبع لديه كان إشارة صغيرة مخفية جيداً، لا تظهر إلا عند الدخول إلى محالّ المتجر. والإسهاب اللغوي الموجود في الإشارة يوضح أن الخيار الوحيد المتاح هو الخروج، أي إذا لم تكن ترغب بالاشتراك، فلديك خياران: إما ألا تدخل إلى المتجر، أو أن تُطفئ هاتفك الخلوي. أما البيانات المجموعة من خلال خدمات كهذه فيمكن، بل وسيتم، تخزينها إلى الأبد. أي إنه يمكن لمحامي زوجتك المصرة على الطلاق أن يستدعي نوردستورم ويوكليد إلى المحكمة للتأكد من أنك وعشيقتك كنتما في المتجر نفسه معاً تشتريان

احتياجاتكما الخاصة. وسيكون رئيسك في العمل قادراً على التعاقد مع سماسرة البيانات للعثور على مكانك في ذلك اليوم الذي اتصلت به لتبلغه بأنك مريض: "إن كنت مريضاً حقاً، فلماذا كنت (ومعك هاتفك) في السينما مع الفتيات ذلك المساء؟". الأسوأ من ذلك، أن المجرمين سيتمكنون من الوصول إلى كل هذه المعلومات مع مرور الوقت من خلال الأوساط السرية الرقمية وسيستخدمونها للابتزاز والرشوة ومطاردة الأهداف التي يختارونها.

حتى منتزه ديزني لاند "المكان الأكثر سعادة على الأرض"، يتحول إلى التقنيات المعتمدة على تحديد المواقع ليلاحق زائريه مستخدماً في ذلك أساور تدعى ماجيك باندس، أو الأساور العجيبة، وهي أجهزة مزودة برقاقات معرفات راديوية تسمح لديزني بتتبع موقع زائريه في كافة أنحاء حدائقه، بهدف استخدام البيانات الكبيرة لأعظمة مدة بقائك في المملكة الساحرة. ومع بدء ديزني بذلك، لا بد أن كثيرين سيسلكون هذه الطريق، ويمكنك أن تتوقع انتشار مثل هذه التقنيات في الكازينوهات والملاجئ وحتى في المطارات في المستقبل.

طقس غائم أمامنا

بالرغم من الكميات الهائلة من البيانات التي يتم تسريبها من هواتفنا، فإن المخاطر الأكثر إثارة للقلق في ما يتعلق بالبيانات الكبيرة تأتي من "الحوسبة السحابية". ويقصد بالسحابة تلك الشبكة الهائلة من موارد الحوسبة المتوفرة على الإنترنت، وإلى استخدام تلك المخدمات البعيدة لتخزين وإدارة ومعالجة معلومات العالم. فالنموذج السائد في الحوسبة يتغير بحيث يصبح قدر أقل من المعلومات يخزن محلياً ليتم التخزين بشكل أساسي في مواقع أخرى على الأرض. فقد بتنا في معظم الأحيان لا نشتري البرمجيات بل نستأجرها أو نحصل عليها للاستخدام المجاني في إطار

نموذج تجاري جديد يُعرف باسم البرمجيات كخدمة، أو ساس.

وعلى جبهة الحوسبة الشخصية، تعني الحوسبة السحابية أن غوغل يخزن رسائلنا وإنستاغرام يخزن صورنا ودروب بوكس يخزن وثائقنا، ناهيك بما تحمله وتقدمه هواتفنا النقالة إلى السحابة من أجلنا. وفي العالم التجاري، لا تستخدم الشركات العميلة دروب بوكس فقط، بل باتت تكلف أطرافاً خارجية من مزودي ساس مثل Salesfoce.com وZoho.com وBox.com، بالمهام التجارية الأساسية التي كانت في السابق تعالجها داخلياً. وفي المجال الجنائي والأمني، يعني تجميع هذه الكميات الهائلة جداً من البيانات، والتي تقدر حجومها بالإكزابايتات، أن أكثر معلوماتنا خصوصية لم تعد تُخزن على أجهزتنا المحلية فقط بل أصبحت الآن تُجمّع على مخدمات الحواسب حول العالم. وبتجميع البيانات الهامة، المالية منها وغيرها، الخاصة بالجميع على مخدمات الحواسب السحابية، لم تعد هناك حاجة إلى قيام المجرمين باستهداف كل جهاز على حدة، وبدلاً من ذلك نضع كافة الجواهر في مكان واحد يستهدفه المجرمون والقراصنة، ولنتذكر هنا ويلي سوتون وحبه للبنوك.

أتت السحابة إلينا لتبقى، وعند هذه النقطة لا مجال للتراجع. ففي بداية عام 2014، خفّض غوغل أسعار عروض التخزين السحابي بنسبة بلغت حوالى 70 بالمئة، لتعادل 0.026 دولاراً لكل غيغابايت في الشهر (أي أقل من ثلاثة سنتات، بينما كانت قيمتها سنة 1980 هي 437,000 دولار). وولدت هذه الحركة موجات من الصدمة في أوساط هذه الصناعة، ونشبت حرب أسعارٍ دخل غمارها عمالقة التخزين السحابي مثل أمازون وميكروسوفت. ومن شأن توفر مثل هذه المصادر الرخيصة للحوسبة، ومع طيف متنامٍ من عروض ساس سيكون له أثر إيجابي هائل على الإنتاجية الشخصية، والمبادرة والإبداع، ما سيؤدي بدوره إلى تسريع الانتقال المحتوم إلى الحوسبة

السحابية. لكن مع هذا التوجه نحو تخزين كافة البيانات المتوفرة في السحابة تبرز مخاطر إضافية. ولنتذكر هنا الاختراقات الضخمة التي حدثت حتى الآن، متاجر تارغيت وهارتلاند لأنظمة التسديد وجي.تي.إكس وسوني بلاي ستيشن. فجميع هذه السرقات لمئات ملايين الحسابات كانت متاحة لأن الانتقال إلى السحابة يعني أن كافة البيانات كانت تُخزن في موقع افتراضي. فالسحابة مريحة لكل من الأفراد والشركات والمجرمين على حد سواء.

إن عمليات الإدارة الافتراضية والتخزين لكل هذه البيانات في غاية التعقيد، وتثير طيفاً واسعاً من من القضايا الأمنية والسياسية والقانونية. فأولاً، أين تقوم هذه السحابة السحرية بتخزين بياناتي بالضبط؟ فعندما يتفحص معظم المستخدمين حساباتهم على الفايسبوك أو يحمّلون صورة على بينتيريست، ليست لديهم أية فكرة حول المكان الدقيق لتخزين هذه المعلومات في العالم الحقيقي. ويتبين من عدم أخذنا لحظة لطرح هذا السؤال كم هذا النظام مريح وغامض في آن معاً. لكن من منظور السيادة المؤسسية والأخطار الشخصية، ثمة فرق كبير بين أن يتم تخزين بياناتك على مخدم في أميركا أو روسيا أو الصين أو أيسلندا.

بدأت الحدود المؤسسية أو الفردية التي تُسْتخدم لحماية معلوماتنا من الداخل بالتلاشي، وبدأت بداية ونهاية شبكات حواسبنا أقل تحديداً بكثير. وتحديد البيانات الداخلة إلى الشركة والصادرة عنها يصبح أكثر صعوبة، وتصبح المهمة شبه مستحيلة على الجبهة الشخصية. فالتحوّل إلى السحابة سيغير قواعد اللعبة من الناحية الأمنية، لأنه يعيد من جديد تعريف أمكنة تخزين البيانات وتحركها ومعالجتها، ما يخلق فرصاً جديدة هائلة للقراصنة المجرمين. علاوةً على ذلك، يثير التخزين غير المحلي لبياناتنا أسئلة مهمة حول اعتمادنا العميق على أنظمة المعلومات السحابية. فعندما تنهار هذه

الخدمات أو تصبح غير متوفرة بسبب هجمات حجب الخدمة، أو عندما تفقد اتصالك بالإنترنت، عندها تصبح بياناتك غير متوفرة وتبقى بالتالي خارج السوق.

كما اكتشف ماتّ هونان، فإن إيداع المعلومات الشخصية القيمة، مثل صور طفل أحدهم وسنوات من البريد الإلكتروني، في عهدة مزودي الخدمات السحابية له مخاطره الخاصة. فكافة مزودي الخدمات السحابية الكبار سبق أن كانوا هدفاً لهجمات إجرامية، ومن بين هؤلاء شركات دروب بوكس وغوغل وميكروسوفت، وعلينا بالتأكيد توقع المزيد في المستقبل. في الحقيقة، بعد مرور عدة سنوات من تعرض هونان للهجوم ونشره مناشدة "للقضاء على كلمة السر" نظراً لفعاليتها شبه المنعدمة، لا يزال الآلاف من الأفراد والشركات يجدون حساباتهم السحابية وقد اخترقت وبياناتهم قد سرقت، ومن بين هؤلاء عدد من ممثلات هوليوود المشهورات. في أواخر عام ،، تعرضت مئات الصور، وكثير منها شخصي جداً أو يتضمن عرياً، العائدة إلى عدد من المشاهير، مثل جينيفر لورانس وكيت أبتون، للسرقة عندما نجح قراصنة باختراق أسماء المستخدمين وكلمات السر والأسئلة الأمنية التي تحمي حساباتهم على أبل آي كلاود. بالرغم من أن مزود الخدمة السحابية هو الذي يتعرض للهجوم، أنت هي الضحية والبيانات المسروقة هي بياناتك. وبالطبع فإن الحقوق المنصوص عليها في شروط الخدمة تقول إن الشركات تكاد لا تتحمل أية مسؤولية عندما يحدث اختراق للبيانات. لكن هذه الهجمات تهدد الملكية الفكرية وبيانات الزبائن وحتّى المعلومات الحكومية الحساسة.

في عام 2008، وُجدت مواصفات التصميم عالية السرية لطائرة الرئيس العمودية مارين ون متوفرة مجاناً على الإنترنت، تستضيفها شبكة زوجية (بي.2.بي) في إيران. تتيح هذه الشبكات الزوجية مشاركة الملفات بسهولة

ولامركزية، وعادة ما ترتبط بتوزيع الأفلام والموسيقى المُقرصنة في الأوساط الرقمية السرية. فكيف أمكن للمخططات والميزات السرية للغاية والخاصة بأكثر المروحيات تطوراً تقانياً في العالم أن تنتهي بيد الإيرانيين؟ إنه أمر بسيط. قرر متعاقد عسكري في بيثيسدا في ولاية ميريلاند يعمل في مشروع مارين ون أنه يستمتع بالموسيقى المجانية على حاسوبه المحمول الخاص بالعمل. وعندما قام بتنزيل برنامج المشاركة الخاص بالشبكات الزوجية، قام بالصدفة ومن دون علم بتنصيب البرنامج في مكان خطأ على حاسوبه. نتيجة لذلك، تسربت المخططات وميزات الحماية الدفاعية للمروحية العسكرية التي تنقل الرئيس من البيت الأبيض إلى الطائرة الرئاسية إلى الشبكات الزوجية لمشاركة الموسيقى حول العالم، وأيضاً إلى إيران. نتيجة للرغبة إلى الاستماع إلى الموسيقى المجانية، تم اختراق مشروع عسكري تكلفته مليار دولار، ومخطط المروحية سيكورسكاي VH-3D الخاصة بالرئيس انتهى بيد شبكة زوجية في إيران تستضيفه إلى جانب أغاني مقرصنة، لكل من مايكل جاكسون وشادميهر أغيلي، ملك البوب الإيراني الذي لا ينازع. واعترف المتعاقد العسكري السابق بخطئه بعد التحقيق معه من قبل مكتب التحقيقات الفدرالي ووزارة الدفاع، ولكن الضرر كان قد وقع. مع اتصالاتنا البينية الشاملة والتخزين المستمر بلا نهاية للمزيد والمزيد من البيانات تصبح التسريبات شيئاً لا مفر منه. فما هي البيانات التي تسربها أنت أو شركتك إلى السحابة؟

بيانات كبيرة، أخ كبير

من اللافت أن الحكومات ليست ضحية لتسريب البيانات وحسب، بل هي سبب العديد منها أيضاً. فالمعلومات هي المحفز لكافة العمليات الاستخبارية، والحكومات بكافة حجومها تستهدف البيانات الكبيرة بشراسة. فليس الصينيون فقط هم من يمارس القرصنة في العالم، بل أيضاً

الأميركيون والبريطانيون والروس والأستراليون والكنديون والسوريون والإسرائيليون والمصريون والإيرانيون، بل وحتى الإثيوبيون. في الحقيقة، يوجد أكثر من مئة بلد لديه برامج اختراق حاسوبي نشطة، وإن لم تكن بدرجة توسع الحكومة الأميركية ووكالة الأمن القومي. ففي كل يوم تقوم وكالة الأمن القومي وفقاً للتقارير باعتراض وتخزين أكثر من 1.7 مليار رسالة بريد إلكتروني ومكالمة هاتفية ورسالة نصية، وهي تجمع قاعدة بيانات تحتوي على حوالى 20 تريليون مناقلة منذ أحداث الحادي عشر من أيلول. وتسجل الوكالة من يتصل بمن، ومن يرسل رسائل نصية أو رسائل بريد إلكتروني لمن ومن يرسل المال لمن.

إلا أنه نظراً للنمو الأسّي في البيانات الكبيرة التي تمتلكها الوكالة، فإن وكالة التجسس الإلكترونية بدأت تستنفد مساحة التخزين المتوفرة لديها. واستجابةً لذلك، تعمل الحكومة حالياً على بناء مرافق عملياتية جديدة واسعة في أقاصي صحراء أوتا، ستسمح لوكالة الأمن القومي بتخزين ومعالجة حجم بيانات أكبر بـ 100,000 مرة من البيانات التي تمتلكها في الوقت الحالي في مكتبة الكونغرس. وما هذه سوى البداية فقط...

وثّقت الأشياء التي كشف عنها إدوارد سنودين العدد الواسع من قنوات البيانات، التي كانت وكالة الأمن القومي تلاحقها، ومن بينها الكميات المتزايدة دوماً من التفاصيل الاجتماعية والجغرافية التي نولدها نحن. قد تكون القائمة التي قدمها سنودين أطول بكثير من أن ندرجها هنا، لكن استعراض العناوين الرئيسية التي أُطلقت حتى الآن كفيل بتوضيح أن القطاع الخاص ليس الوحيد في سعيه الشرس خلف البيانات الكبيرة. إذ يسمح برنامج بريزم التابع لوكالة الأمن القومي للحكومة بجمع كميات غزيرة من البيانات من شركات، مثل ميكروسوفت وغوغل وفايسبوك وسكايب وأميركا أون لاين وأبل، من بينها بيانات البريد الإلكتروني

للمستخدمين وفيديوهاتهم وصورهم وتحديث حالاتهم ومواقعهم.

كشف سنودين أيضاً أن وكالة الأمن القومي قامت بالدخول ومن ثم تنزيل جهات الاتصال المتبادلة بين مستخدمي وسائل التواصل الاجتماعي (أي مع من يتحدثون وكم مرة وأين هي مواقعهم)، ومن ضمنها أيضاً الشبكات الاجتماعية للمواطنين الأميركيين. وأضيفت إلى هذه التسجيلات ملايين القوائم من جهات الاتصال ومذكرات العناوين التي جمعتها بدورها الوكالة. أي إنك عندما تختار استخدام غوغل كونتاكتس أو آيكلاود لتخزين التفاصيل الشخصية لأصدقائك وأفراد عائلتك وزملائك في العمل، فإن هذه التفاصيل يمكن بسهولة أن تُستهدف وتُغنم من قبل الآخرين بمن فيهم الحكومات.

لا ترتبط وكالة الأمن القومي بعلاقات تعاون مع الشركات الأميركية وحسب، بل إنها تستهدف أيضاً هذه الشركات في الوقت المناسب، ومن ضمنها غوغل وياهو!، التي اخترقت الوكالة الجاسوسية مراكز بياناتها دون ترخيص مسبق. فباستخدام التقنيات نفسها التي يوظفها القراصنة وعصابات الجريمة المنظمة، قامت وكالة الأمن القومي بنشر برمجياتها الخبيثة في أكثر من خمسين ألف شبكة حاسوبية حول العالم، لكي تتمكن من الدخول إلى أهداف تهمّها. بل إن الوكالة قامت أيضاً بانتحال شخصية الفايسبوك في عددٍ من هجمات الوسيط لتتعقب الأفراد عبر الشبكات الاجتماعية. وتقوم هذه التقنية على جعل الأهداف تتصل من خلال نسخة للفايسبوك خاضعة للحكومة، ما يسمح للوكالة بتنزيل برمجيات خبيثة على أجهزة هذه الأهداف.

لم تقم وكالة الأمن القومي بهذا العمل لوحدها، بل تعاونت مع منظمات شقيقة مثل مقابلتها البريطانية ومركز قيادة الاتصالات الحكومي. حيث اشتركت هذه الوكالات معاً في برنامج أوبتيك نيرف، الذي كان يعترض ملايين

فيديوهات المحادثة على ياهو! عن طريق التحكم بكاميرات الفيديو الموجودة في الحواسب المحمولة للمشتركين والتقاط صور كل خمس دقائق. تم تخزين ملايين الصور من بينها عدد كبير من الصور الجنسية الواضحة التي تتضمن عرياً. والمروع هو أن معظم فيديوهات المحادثة التي تم اعتراضها كانت لأشخاص، ليس الغرض من استهدافهم هو عملية استخبارية، بل لأنه كان من الأسهل الاستحواذ على كافة المحادثات بدلاً من اختيار الفيديو الواجب الاحتفاظ به بشكلٍ فردي.

استنسخت وكالة الأمن القومي أيضاً التقنيات السابقة التي أثبتت جدارتها لدى المعلنين والمسوقين، وفي عمليات جمع البيانات التجارية. فقد قامت الوكالة الجاسوسية على سبيل المثال بإنشاء وتنزيل ملفات كوكيز للتتبع على الأقراص الصلبة والهواتف النقالة، لتسجيل المواقع والعادات الشبكية لأولئك الخاضعين للمراقبة. ووفقاً لسنودين، كانت وكالة الأمن القومي أيضاً تستغل تطبيقات الهواتف الذكية، مثل لعبة الطيور الغاضبة من شركة روفيو. فقد أدركت الوكالة الجاسوسية أن الطيور الغاضبة كانت تبلي أصلاً بلاءً حسناً في سرقة البيانات، لذلك لم تكن الوكالة بحاجة إلى تكليف نفسها عناء تكرار العمل المنجز سلفاً. بدلاً من ذلك، قامت الوكالة فقط باعتراض الكميات الضخمة من البيانات التي كانت ترسل أصلاً إلى شركة روفيو من قبل أولئك الذين كانوا يظنون بسذاجة أن غرض التطبيق الحقيقي هو فقط التسلية من خلال رمي الطيور على الخنازير الخضراء الضاحكة.

أدركت نسبة قليلة جداً من مستخدمي لعبة أنغري بيردس البالغ عددهم 1. مليار مستخدم، أن تطبيقهم المجاني كان يقوم بمشاركة بياناتهم مع شركة روفيو، ابتداءً من موقعهم الدائم ووصولاً إلى ميولهم الجنسية. لكن ما لم يدركه أحد، حتى الشركة المنتجة لهذا التطبيق، هو أنهم يقدمون هذه

البيانات (دون إدراك بالطبع) إلى وكالة الأمن القومي أيضاً. بل إن محللي البيانات في وكالة الأمن القومي كانوا يستخدمون أدوات التجسس التابعة للوكالة لاستهداف أصدقائهم أو صديقاتهم أو أزواجهم أو زوجاتهم أو عشاقهم السابقين. وقد تم توثيق العديد من الانتهاكات حين كان بعض موظفي الوكالة يدخلون إلى عناوين البريد الإلكتروني وأرقام هواتف هؤلاء الأشخاص، لكي يقرأوا بريدهم الإلكتروني ويتتبعوا مواقعهم ويستمعوا لمكالماتهم الهاتفية. أثارت هذه الأعمال الفردية الصادرة عن الموظفين سؤالاً بليغاً وهاماً في آن معاً هو من يراقب المراقبين؟

فيما الغالبية الساحقة من أهداف الوكالة تبدو بعيدة ما وراء البحار، فإن عشرات الأجهزة الأمنية في أنحاء العالم تستخدم التجسس الإلكتروني لمراقبة وقمع مواطنيها المحليين. ففي الصين وإيران ومصر وسوريا والبحرين وغيرها من البلدان تتم مراقبة واعتراض البيانات المخزنة على الإنترنت باستمرار، لأسباب تتعلق بالاستخبارات السياسية وللحفاظ على استقرار الوضع الراهن. ومعظم هذه البلدان لا تنتج أنظمة مراقبة كهذه، بل تشتريها من شركات في دول أخرى، مثل الشركة الألمانية غاما إنترناشونال، مُصنّعة حزمة أدوات المراقبة الإلكترونية فينفيشر، التي تسمح لأجهزة الاستخبارات المحلية بمراقبة آلاف الأهداف بالتزامن عن طريق الهواتف النقالة وشبكات الوسائط الاجتماعية والنشاطات على الإنترنت.

حين يتم إعداد أنظمة مُراقبة البيانات الشاملة هذه، يمكن استخدامها في سبيل الخير العام، كإيقاف اعتداء إرهابي وشيك، أو في سبيل الضرر العام، كقمع ومضايقة نشطاء حقوق الإنسان وتعطيل العملية الديمقراطية. ففيما قامت الوسائط الاجتماعية بالكثير من أجل دعم الثائرين في مصر وتونس خلال الربيع العربي، إلا أن القصة التي استقطبت اهتمام الصحافة في العالم هي الوجه المعاكس تماماً لهذه البيانات الاجتماعية. فقد شكلت ملايين

التغريدات والكتابات على فايسبوك أدواتٍ مفيدة للحكومات لملاحقة منتقديها. وتنظيم احتجاج على فايسبوك يعطي الحكومة نظرة واضحة ومقربة عمّا تخطط له النشاطات المعارضة، وتتوفر لدى كافة الحكومات تقريباً المهارات اللازمة للاستفادة من هذه البيانات المسربة.

في الثورة التي قامت ضد بشار الأسد وبدأت عام 2011، طورت الحكومة السورية، بمساعدةٍ ودعم تقني من إيران، برامج متنوعة لمراقبة مواقع التواصل الاجتماعي مثل فايسبوك وتويتر لتتبع الاتصالات بين شخصيات المعارضة. وتم تحديد ومهاجمة قادة الحركة المناهضة لنظام الأسد وكذلك أفراد عائلاتهم. وفي الأيام الأخيرة من حكم الرئيس السابق فيكتور يانوكوفيتش، برهنت قواته الحكومية على قدرة التكنولوجيا على قمع وإخضاع قوات المعارضة. فعندما كان المتظاهرون يتجمعون في شوارع العاصمة كييف، كانت الحكومة الأوكرانية تتحرى مواقع جميع الهواتف النقالة القريبة من الشوارع التي تجري فيها الصدامات بين شرطة مكافحة الشغب وبين الثائرين. كان تحديد الهواتف النقالة (وأصحابها) يتم بالزمن الحقيقي ليتلقوا ما يمكن اعتباره أكثر الرسائل سخرية على الإطلاق يتم إرسالها من قبل حكومة: "عزيزي المشترك، لقد تم تسجيلك كمشترك في شغب جماعي"، في لغة منتقاة بعناية نظراً لقيام يانوكوفيتش بتجريم مثل هذه المشاركة قبل ذلك بأيام بما يعرض أي شخص مخالف إلى الاعتقال الفوري

الوجه المظلم للبيانات الكبيرة

قد يكون الإرث الأهم الذي ستتركه للبيانات الكبيرة هو أحد الأمور التالية: المراقبة الدائمة أو إلغاء الخصوصية أو موجة من التهديدات الإجرامية التي لم يسبق تخيلها. فمواقع التواصل الاجتماعي والهواتف الذكية وتطبيقاتها والسحابة وغيرها من التكنولوجيات، تعني أن

نوردستورم وأكسيوم وفايسبوك وغوغل ليست وحدها القادرة على إيجادك متى تريد، بل أيضاً مجموعات مثل زيتاز ولاشكار إي طيبة، والمتعسفين المنزليين واللصوص. والشيء الذي لا يدركه معظم الناس هو أن أية مجموعة من البيانات ستتسرب ذات يوم. فأمن أنظمتنا الحاسوبية الحالية أضعف من أن يضمن تخزين كميات المعلومات التي ننتجها بأمان.

اقتصرت التهديدات الرئيسية للبيانات الكبيرة حتى اليوم على إمكانيات السرقة والتسريب. لكن تلك ليس سوى البداية. فمع تقدم الزمن، سنواجه مخاطر قد يثبت أنها أشد مما عرفناه بعد، وتتمثل في التعديل غير الشرعي للمعلومات التي يعتمد عليها العالم لتسيير نشاطاته اليومية. فبالرغم من أننا وضعنا ثقة كبيرة في البيانات التي كنا نكدسها بحميّة، فإن الدقة المفترضة لهذه المعلومات، كما سنكتشف، يمكن بسهولة تخريبها، الأمر الذي سيكون له عواقب واضحة تطال الجميع. فتماماً كما يمكن للأشرار سرقة بياناتنا، بإمكانهم أيضاً تغييرها. ستتركنا هذه العاصفة التي تلوح في الأفق ضعفاء وستزعزع مصادر إيماننا في العالم القائم على البيانات بطرقٍ لم يقم أحد بإعطائها حق قدرها حتى الآن.

الفصل الثامن
إنما إيماننا بالشاشة

لم يعد العالم يُدار بالأسلحة أو الطاقة أو المال، بل بواسطة الآحاد والأصفار، أي ببتّات البيانات، وما هذه سوى إلكترونات. ثمة حرب مستعرة، حرب عالمية. وليس المهم من لديه الكم الأكبر من الرصاص، بل المهم من يسيطر على المعلومات، أي على ما نراه وما نسمعه وعلى أساليب عملنا وتفكيرنا. إنها حرب المعلومات.

على لسان كوسمو (بين كينغسلي)، في "الوغد ذو الأحذية الرياضية"

تم فحص جميع الأنظمة. كان هنالك خمسة آلاف جهاز طرد مركزي تعمل في مفاعل ناتانز لتوفير الطاقة النووية في إيران، وكانت الجمهورية الإسلامية تحقق تقدماً في برنامجها "السلمي" للطاقة النووية. وإذا استمر السير على هذا المنوال، فستتوفر لدى إيران قريباً الكمية الكافية من اليورانيوم المخصب 235 لإقامة محطة طاقة نووية خاصة بها أو لبناء أول قنبلة ذرية لها، تبعاً للطرف الذي تسأله. وبالرغم من أن إيران كانت دوماً تؤكد أن لا غرض من نشاطاتها النووية سوى الاستخدام المدني للطاقة، فإن معظم دول العالم، بما فيها الولايات المتحدة وأوروبا وإسرائيل، بل وحتى الأمم المتحدة، لم تكن مقتنعة بذلك.

وجدت الوكالة الدولية للطاقة الذرية التابعة للأمم المتحدة عام 2005 أن إيران لا تلتزم بمعاهدة وقف انتشار الأسلحة النووية التي وقّعت عليها، وقدمت وكالة التفتيش تقريراً إلى مجلس الأمن تعرب فيه عن قلقها إزاء الأمر. واستجابت الأمم المتحدة بأن طالبت إيران بتعليق نشاطاتها النووية في ناتانز، ليرد عليها رئيس إيران في ذلك الوقت محمود أحمدي نجاد برفض قاطع. وختم موظفون رفيعو المستوى في الوكالة تقريرهم، بالقول إن لدى إيران معلومات كافية لتصميم وإنتاج قنبلة ذرية قابلة للاستخدام، ونتيجة

لذلك تم فرض عقوبات دولية على إيران. لكن هل ستمنع العقوبات إيران من الحصول على القنبلة؟ نظراً لموقع إيران المتقدم على القائمة الأميركية لـ "محور الشر"، لا بد من فعل المزيد.

ثمة أسباب سياسية تحول دون توجيه ضربة عسكرية مفتوحة، لكن الرئيس الأميركي جورج دبليو بوش سمح في السنة التالية بهجوم سري على المنشآت النووية في ناتانز، ولقب برنامج العملية السري هذا باسم الألعاب الأولمبية، وفقاً لصحيفة نيويورك تايمز. وكانت النتيجة "أفضل تلاعب سري بالطيف المغناطيسي - الكهربائي منذ الحرب العالمية الثانية عندما قام محللو الشفرات في ذلك الوقت باختراق شفرة آلة الإنيغما ما سمح لهم بفك الشفرات النازية".

لم يكن الإيرانيون لقمة سائغة، وكانوا أذكياء بما فيه الكفاية لكي لا يضعوا المعلومات القيّمة الخاصة بالجمهورية الإسلامية على الإنترنت. لذا فإن منفذي عملية الألعاب الأولمبية لم يتمكنوا من إيجاد طريق ضعيف الحماية يقودهم إلى الطريق السريع الأكبر للمعلومات. وكان لا بد لإنجاح الخطة من جمع شبكة من العملاء والمهندسين وعمال الصيانة، سواءٌ كجواسيس أو كمساعدين غافلين، والتنسيق بينهم بدقة هائلة. أما السلاح الذي اختير لتنفيذ هذه العملية السرية فكان عبارة عن ذاكرة يو.إس.بي.

لتخريب أجهزة الطرد في ناتانز، تم ابتداع نوع جديد من الأسلحة الإلكترونية، وهو نوعٌ يمكنه الانتقال من العالم الافتراضي للحواسب ليدخل بالعالم المادي لأنظمة التحكم الصناعية. كان فيروس إنتر ستوكسنيت دودة حاسوبية متطورة جداً يُعتقد أنها أُنشئت من قبل الولايات المتحدة وإسرائيل لإبقاء عدوهم تحت السيطرة. قام مخترعو ستوكسنيت بنسخ الفيروس على ذاكرة يو.إس.بي بسيطة. بعد أن تم تحميلها وقفلها، باتت الشريحة جاهزة للبحث عن فريستها. أما كيف تم تهريب الذاكرة إلى

ناتانز ومن أدخلها إلى شبكة حواسب المنشأة، فهي أسئلة بقيت بلا جواب حتى الآن.

ما هو معروف، على أية حال، هو كيفية انتشار البرمجية الخبيثة بسرعة عبر البنية التحتية لتكنولوجيا المعلومات في المحطة. فمجرد إدخال الذاكرة عبر منفذ يو.إس.بي لأحد الحواسب، كان كفيلاً بإصابة نظام تشغيل مايكروسوفت ويندوز عبر استغلال ثغرة من نوع "اليوم صفر" لم يكن قد تم توثيقها من قبل. واستخدمت الدودة رخصة أمنية رقمية مزورة أيضاً تدعي أنها موثوق ومصدقة، ما سمح لها باستنساخ نفسها كما يحلو لها عبر بنية المعلومات التحتية في منشأة ناتانز. وبينما كانت الدودة تنتشر من حاسب إلى آخر ومن شبكةٍ إلى أخرى، كانت تطرح سؤالاً بسيطاً على كل جهاز تصيبه: هل هذا الحاسب متصل بنظام تحكم صناعي مصنّع من قبل شركة سيمنز الألمانية المتعددة الجنسيات؟

أنجز الأميركيون والإسرائيليون مهمتهم وأصبحوا يعرفون أن أجهزة الطرد المركزي في منشأة ناتانز كانت تعمل بنظام التحكم المنطقي الصناعي القابل للبرمجة من سيمنز S7-417، كان يراقب الصمامات وأجهزة استشعار الضغط الخاصة بأجهزة الطرد المركزي. أما الحواسب غير المتصلة عبر برنامج سيمنز، فكانت الدودة تخفق في التكاثر فيها وتتلاشى. أما حين تكتشف دودة ستوكسنيت حاسباً أو شبكةً تعمل ببرنامج سيمنز، فإن السلاح الإلكتروني يبدأ عمله بنشاط شاقاً طريقه من حاسب ويندوز إلى نظام التحكم لصناعي الذي ينظم عمل أجهزة الطرد المركزي الإيرانية.

كان منفذو الهجوم يعلمون أن عملية تكرير اليورانيوم U-235 كانت عملاً مخادعاً. فأجهزة IR-1 للطرد المركزي المستخدمة في ناتانز مصممة لتدور بسرعة 100000 دورة في الدقيقة، وهو عمل جبار من حيث السرعة والتقانة المستخمة. فحين تدور أجهزة الطرد المركزي دوراناً أبطأ من اللازم،

لا يتم فصل اليورانيوم الضروري للطاقة النووية (والقنابل) بشكلٍ مجدٍ. أما إذا كان دورانها أسرع من اللازم، فإنها تبدأ بالاهتزاز بشكلٍ خارج عن السيطرة إلى أن يصبح الضغط مرتفعاً جداً، فينفجر المحرك ما يتطلب تبديل جهاز الطرد. ومن دون أجهزة الطرد لا وجود للطاقة ولا وجود بالتالي للقنابل، والنتيجة انتهاء التهديدات.

كان برنامج سيمنز هو مفتاح الهجوم، لكن مخترعي ستوكسنيت لم يكونوا محاربين إلكترونيين طائشين تميل عقليتهم إلى النهب والتدمير. بل كانوا صبورين ومخططين استراتيجيين وأذكياء في هجومهم على ناتانز. ففي المرحلة الأولى من الهجوم، لم تقم دودة ستوكسنيت بشيء سوى المراقبة والمكوث بصمت مع قيامها سراً بجمع المعلومات لتطلع على كيفية عمل أجهزة الطرد المركزي. وكانت الدودة تسجل كافة اكتشافاتها بحركة متقنة مُعدّة مسبقاً ستثبت أهميتها الحاسمة في نجاح العملية.

ففي المرحلة الثانية من العملية، بدأت ستوكسنيت بإظهار قواها الحقيقية عندما فرضت سيادتها على أنظمة التحكم الصناعي في ناتانز. وبدأ سادة الدمية تدريجاً بالتلاعب بمحركات وصمامات أجهزة الطرد المسؤولة عن تخصيب اليورانيوم في المنشأة، وراحوا على مدى أشهر، بل حتى سنوات، يقومون بتسريع وإبطاء أجهزة الطرد لتتذبذب عن الشكل الذي صممت عليه وهو 100000 دورة في الدقيقة. فكان ضغط أجهزة الطرد يرتفع والدوارات تتوقف، فبدأت كميات اليورانيوم المخصب بالانخفاض.

في هذه الأثناء، داخل غرفة التحكم بالعمليات العالية التأمين في ناتانز، كانت جميع الأنظمة تعمل وفق جدول العمل، على الأقل كما كان يظهر على شاشات الحواسب التي يراقبها المهندسون في المنشأة. فكان لكل واحد من آلاف أجهزة الطرد ضوء يمثله على شاشة الحاسب يشير إلى أي خلل في

النظام. فكان الضوء الأخضر يعني أن أجهزة الطرد تعمل بشكلٍ طبيعي، أما الرمادي أو الأحمر فيشيران إلى مشكلةٍ ما. كان المهندسون يراقبون شاشاتهم يوماً بعد يوم بإخلاص بحثاً عن أي مؤشر لمشكلة ما. لكن الأضواء بقيت خضراء في أنظمة حماية البيانات التي أمامهم. نظام الحماية التسلسلي؟ بخير. ضغط أجهزة الطرد؟ بخير. سرعة المحركات؟ بخير. الشاشات على الجدران وشاشات الحواسب وشاشات لوحات التحكم، كانت كافة أنظمة المعلومات داخل مركز قيادة العمليات تقول للإيرانيين إن طموحاتهم النووية تسير في طريقها. إلا أن ذلك كان أبعد ما يكون عن الحقيقة.

كان الضرر الذي يسببه فيروس ستوكسنيت مصمماً بحيث يبقى بعيداً عن الأضواء في البداية. لكن تدريجاً، بدأت بعض أجهزة الطرد المركزي تدور على نحو خارج عن السيطرة، لكن الإيرانيين ألقوا اللوم في هذه المشكلات على مهندسيهم غير الأكفاء. وكان لكل جهاز طرد يتوقف تفسير مختلف: فهذا الجهاز كان بطيئاً جداً، أما الآخر فكان سريعاً جداً، أما هذه الأجهزة هناك فالضغط فيها عالٍ جداً. وكان اليورانيوم المُعَالج من نوعٍ سيئ وغير صالح للاستخدام. واستمرت عمليات الفحص في المنشأة مراراً وتكراراً، وتابع الباحثون مراقبة سير العمليات كافة عبر الحواسب داخل غرفة التحكم. ومع مرور الوقت، بدأت العشرات ومن ثم المئات من أجهزة الطرد بالتوقف. وباتت الطموحات النووية الإيرانية الآن موضع شك. فما الذي كان يجري؟ كل ما في الأمر هو أن الإيرانيين بالغوا في ثقتهم بشاشات الحواسب التي تتحكم بموقع التخصيب النووي السري الثمين.

كان لعملية تجميع البيانات والتسجيل الحاسوبي لأنظمة التحكم الصناعي، والتي نفذها فيروس ستوكسنيت بسرية في المرحلة الأولى من الهجوم، هدف واضح، وإن لم يكن بديهياً في البداية، وهو توثيق مجريات

برامج سيمنز بشكل كامل وهي في حالة عمل طبيعي كامل. المحركات تدور وفقاً للخطة والضغط عند المستويات المتوقعة، كافة الأنظمة تعمل، وأضواء الصيانة خضراء. كانت دودة ستوكسنيت تجمع كافة هذه البيانات وتسجلها وكأنها تصور برنامج سيمنز بالفيديو وتحفظ التسجيل بعناية للأجيال القادمة. أما ما حدث بعد ذلك فبدا مستمداً مباشرة من مشهد هوليوودي شهير، تم تصويره عدة مرات في أفلامٍ مثل المحيط الحادي عشر والخزينة الوطنية. حين يقوم المهاجمون ببساطة بتسجيل فيديو مسبق باستخدام الكاميرا لخزنة الكازينو أو لغرفة الخزينة المستهدفة ليعيدوا عرضه على شاشات المراقبين وفريق الأمن.

عندما بدأت أجهزة الطرد المُخصبة لليورانيوم بالدوران خارج السيطرة في ناتانز، قام ستوكسنيت باعتراض قيم البيانات الحقيقية الصادرة عن حساسات الضغط والدوران والاهتزاز قبل وصولها إلى غرفة التحكم بالعمليات التي يراقبها مهندسو المنشأة. وبدلاً من أن يقدم البيانات الصحيحة الصادرة عن برنامج سيمنز بالزمن الحقيقي، كانت دودة ستوكسنيت تقوم ببساطة بإعادة تشغيل المعلومات المسجلة مسبقاً، والتي حصلت عليها في المرحلة الأولى من العملية، والتي تُظهر سير العمليات بشكلٍ طبيعي. وتكفلت هذه الحركة الذكية، على الرغم من أن أنظمة التحكم الصناعية كانت تنصهر وتصرخ رقمياً طلباً للنجدة، باستبدال إشارات اللون الأحمر التي يعرضها النظام بفيض من اللون الأخضر الساكن على شاشات الإيرانيين، الذين كانوا يتولون التحكم بناتانز. وبينما كانت أجهزة الطرد تدور خارج نطاق السيطرة وتنهار، لم يكن المشغلون في غرفة التحكم الرقمية يعلمون أن الواقع الذي يعيشونه واقع مخترق سيطرت عليه دودة تحمل اسماً مضحكاً أُرسلت في مهمة للبحث والتدمير.

الحياة في عالم الوسطاء

لسوء الحظ، ثمة ما يجمع بينك وبين الإيرانيين أكثر مما تدرك. فحتى إذا كنت لا تنتج اليورانيوم، فأنت تعتمد على الشاشات في كل يوم لتفسر العالم الذي يدور من حولك. يخبرك هاتفك الخلوي من اتصل بك، بينما يذكرك حاسبك بضرورة تحديث نظام التشغيل، ويرشدك نظام الموقع الجغرافي في سيارتك على الطريق إلى موعدك الصباحي. يحدث كل ذلك، وأكثر، قبل أن تنهي فنجان القهوة الثاني. أما النتيجة، فهي أننا لم نعد نعيش حياتنا من خلال قدراتنا الشعورية الفطرية، بل نتلقاها عبر وسيط هو الشاشات، هذه الجدران الواقعية التي تفصلنا عن إدراكنا الحقيقي وتعرف لنا العالم. تقف الشاشات وسيطاً بيننا وبين العالم الحقيقي، فتعرض معلومات يزعم أنها مكافئة للواقع، لكنها في أفضل حالاتها مجرد قيمة تقريبية يمكن التلاعب بها بسهولة.

في المطارات والمستشفيات والبنوك وماكينات الصرافة الآلية، أصبحت الشاشات أجهزة دائمة الوجود في حياتنا. لكن الشاشات في الوقت الحالي صامتة، لا تزيد مهمتها كثيراً على تقديم المعلومات الضمنية الموجودة في أنظمة البيانات، والتي من الواضح أنها بدورها عرضة للاختراق. أولئك الذين يتحكمون بشفرة حاسوبنا يتحكمون أيضاً بشاشاتنا، وبالتالي بتجاربنا وإدراكنا. وكل شيء قابل للتلاعب، بدءاً بألعاب الفيديو وانتهاءً بآلات الاقتراع، فأن ترى شيئاً بعينيك أو تسمعه بأذنيك في هذا العالم الجديد لا يعني أبداً أنه قانوني أو صحيح أو آمن، إذ يمكن للشاشات التي نشاهدها أن تخدعنا بطرق لا يزال على كثيرين من أن يدركوها بعد.

سواء أدركت ذلك أم لا، فإن تجربتك في عالم الإنترنت التي تعرض على شاشة رقمية يتم تصميمها لأجلك. وقد تكون بعض عمليات الفلترة مفيدة. فمع وجود مليارات التغريدات وصور سنابتشات وتحديثات الحالة ومدخلات المدونات، ما من أحد منا قادر على استهلاك كمية البيانات التي

نتعثر بها يومياً. وتعمل شركات الإنترنت المدركة لذلك على مختلف المستويات لمعرفة تفضيلاتك، لتصميم تجربتك على الإنترنت مستخدمةً سلسلة من خوارزميات الحاسب. يقوم الفايسبوك بدراسة روابطك على الإنترنت وصورك وملاحظاتك ورسائلك وأحداثك وإعجاباتك ليرتب ما يعرضه على شاشتك كل يوم. لذا فإنك لا ترى كل ما يُكتب من قبل أصدقائك أو على الصفحات التي تتابعها، بينما يشاهد أصدقاؤك على مجرى الأخبار الخاص بهم 10 بالمئة فقط من تحديثاتك التي تجريها. بقدر الجهد الكبير الذي يبذله فايسبوك في دراستك وتفصيلك خدمة للمعلنين، يبذل الموقع قصارى جهده ليحدد منشورات أصدقائك التي تفضل أن تراها في كل مرة تزور فيها موقعه أو تشغّل تطبيقه. لكن لماذا يقوم فايسبوك بذلك؟ ببساطة، تعلم فايسبوك وغوغل وغيرهما من شركات الإنترنت أنها إذا قدمت لك الأشياء الصحيحة التي ترضيك، فإنك ستمضي وقتاً أطول في مواقعها وستنقر على روابط أكثر، ما يسمح لها بتقديم المزيد من الإعلانات لك.

ليس الفايسبوك وحده في هذه اللعبة في أي حال، إذ يقوم غوغل أيضاً بإحصاء عمليات البحث السابقة التي قمت بها، وهذا هو الأهم، ما قمت بالنقر عليه، لكي يفصل تجربة بحث على مقاسك. ففي كتابه "فقاعة الفلاتر" يوثق الباحث في مجال التقانة إيلي باريزَر هذه الظاهرة بدقة. فحصولك على نتائج "صحيحة" هو مجال تجاري كبير، وثمة الملايين من خوارزميات الحواسب المكرسة لهذه المهمة. ووفقاً للتقارير فإن لدى غوغل ما لا يقل عن سبع وخمسين إشارة شخصية منفصلة يتم تتبعها ودراستها قبل الإجابة عن أسئلتك. من بين هذه الإشارات نوع الحاسب الذي تعمل عليه ومحرك البحث الذي تستخدمه والوقت ودقة شاشة الحاسب والرسائل المستلمة على جيميل، والفيديوهات المُشاهدة على يوتيوب

بالإضافة إلى موقعك المادي. يغيّر غوغل نتائج البحث الذي يقدمها بالزمن الحقيقي معتمداً في ذلك على ما يعرفه عنك. فالبحث عن كلمة "إجهاض" يعود بروابط إلى تحديد النسل بالنسبة للبعض وإلى موقع الكنيسة الكاثوليكية بالنسبة للبعض الآخر؛ وإذا كنت تبحث عن كلمة "مصر"، فقد تجد نتائج تتعلق بالربيع العربي، فيما تكون والدتك تطالع معلومات عن الأهرامات أو عن رحلة في نهر النيل. وعلى غرار باريسر، يمكنك أن تجرب بنفسك، وستقدم لك النتائج تصوراً واضحاً عن كيفية رؤية غوغل لك.

لا يوجد في الحقيقة شيء اسمه "غوغل القياسي". وقد اعترف إريك شمديت على الملأ بأنه "سيكون من الصعب على الناس أن يشاهدوا أو يستهلكوا شيئاً (على الإنترنت) إن لم يكن معداً خصيصاً لهم بطريقة أو بأخرى". وفيما ليس من الضروري أن تكون نية خبيثة وراء أي من ذلك، فثمة أسئلة مهمة يجب طرحها عن كيفية اختيار وتخزين ورعاية هذه المعلومات من قبل آخرين يزعمون أنهم يمثلونك. ويبقى التحدي على سبيل المثال في أن غوغل وفايسبوك ونيتفليكس وأمازون لا تنشر خوارزمياتها. بل إن الطرق التي تستخدمها لفلترة المعلومات التي تراها، هي في الحقيقة طرق خاصة بكل شركة تمثل "الوصفة السرية" التي توجه ربحيتها. المشكلة في هذا الأسلوب الخوارزمي الذي يعتمد طريقة "الصندوق الأسود" في التعاطي مع المعلومات، هي أننا لا نعلم ما الذي يتم إعداده لنا في الخفاء أو ما الذي لا نراه. والنتيجة هي أن حياتنا الرقمية، التي تصلنا عبر بحر من الشاشات، تتم معالجتها وفلترتها يومياً بطرق غامضة معمّاة. لا يؤثر هذا التحول الجذري في طريقة تدفق المعلومات على الإنترنت على الطريقة التي تصلنا بها المعلومات وحسب، بل على نظرتنا إلى العالم أيضاً. ومعظمنا يعيش في فقاعات خلقتها عمليات الفلترة دون أن ندرك ذلك.

تعمل الدول في أنحاء العالم أكثر فأكثر على تحديد البيانات التي يُسمح للمواطنين بالدخول إليها والمعلومات التي يجب حظرها. فعبر حجج مقنعة مثل "حماية الأمن القومي" و"ضمان حقوق الملكية الفكرية" و"الحفاظ على القيم الدينية"، والعبارة الخالدة المحبوبة "حماية الأطفال"، تقوم الحكومات بتوسيع جدران النار القومية بهدف مراقبة الإنترنت. وبعض التقنيات المستخدمة في هذه الفلترة مكشوف للعامة. ففي فرنسا وألمانيا، على سبيل المثال، تخضع المواقع التي تشجع النازية أو تنكر المحرقة للرقابة علناً. وفي سوريا، تم اعتراض اليوتيوب والفايسبوك وأمازون وهوتميل ومواقع كردية سابقة. في العديد من الحالات، على أية حال، لا تتم الإشارة إلى مراقبة معلوماتك على الإنترنت، وبدلاً من ذلك، ببساطة لا يظهر مضمون معلوماتك. وفي الإمارات العربية المتحدة، قامت الحكومة بمنع الدخول إلى كل المواقع المنتهية بـ il. والموجودة في إسرائيل، لتلغي رقمياً وجود الدولة اليهودية من العالم الافتراضي.

كانت شركات التقانة تشترك ببرامج المراقبة القومية وتوافق على مطالب الدول بفلترة المحتويات المضرة بالزمن الحقيقي، كما فعل غوغل عندما دخل السوق الصينية عام 2005. لكن ربما لا توجد حكومة تبزّ حكومة الصين في مهارتها وصرامتها في ما يتعلق بفلترة الإنترنت. إذ يضمن برنامج "جدار النار العظيم" للصين عدم قدرة سكانها الذين يتجاوز عددهم المليار نسمة، على الاطلاع على المواضيع السياسية الحساسة، مثل احتجاجات ساحة تيانانمين والتفاصيل الدقيقة عن القيادة الصينية، أو المناقشات التي تتناول حقوق شعب التبت والدالي لاما وفالون غونغ واستقلال تايوان والإصلاح السياسي أو حقوق الإنسان. إلا أن مراقبة الإنترنت لا تقتصر على الطغاة والأنظمة الاستبدادية. ففي عام 2014، كان هنالك أكثر من أربعة مليارات إنسان يعيشون في بلدانٍ تطبق الرقابة على الإنترنت بطريقة أو

بأخرى.

لا تخبرك الشاشات بما يدور حولك حقاً، بل بما تريد لك الحكومة أو الفايسبوك أن تراه. فإذا قمت بالبحث عن شيء ولم تجده، فكيف لك أن تعرف ما إذا كان موجوداً حقاً؟ يمكننا إعادة صوغ سؤال فلسفي قديم: إذا سقطت شجرة على الإنترنت ولم يشر أي محرك بحثٍ إلى ذلك، فهل يمكن للسقوط أن يحدث أي صوت؟ بينما نعيش حياة تزداد فيها وساطة الشاشات، ما لا يوجد على الإنترنت، لا يوجد على الإطلاق. وحين لا يشير غوغل إلى حدثٍ معين، فهذا يعني أنه لم يحدث أبداً. وبالعكس، إذا أشار غوغل إلى حدثٍ ما، فيبقى من الممكن أنه لم يحدث. أهلاً بكم إلى عالم الخداع الرقمي، تلك القاعة الافتراضية من المرايا التي تمثلها الشاشات حيث كل شيء يتحقق بالسحر.

الخطر العميق الذي يتهدد الحياة تقانياً في عالم من الوسطاء هو أن هذا العالم يخلق فرصاً كبيرة للتلاعب بالمعلومات بطرقٍ غير مضبوطة، يعجز معظمنا عن توقعها أو فهمها. فالشاشات تتحرك وتومض في كل مكان من حولنا لتلفت انتباهنا. لكن ماذا لو كانت هذه الشاشات تكذب؟ ماذا لو كانت تقدم لنا معلومات زائفة ومضللة؟ في عالم اليوم، يمكن لكل شيء نراه على الشاشات أن يكون زائفاً ومن السهولة تقليده. اسأل أي شخص كم مرة سبق له أن زار موقعاً للحصول على موعدٍ، فسوف يخبرك أو تخبرك: أن ما تراه ليس دائماً ما تحصل عليه.

لا تحوسب

لماذا، في بعض الأحيان كنت أعتقد بوجود ستة أشياء مستحيلة قبل الإفطار.

لويس كارول، عبر المرآة

ما الذي يجمع بين القراصنة والمحتالين والجريمة المنظمة من جهة، وبين

فايسبوك وغوغل ووكالة الأمن القومي من جهة أخرى؟ يستطيع كل منهم تأدية دور الوسيط والتحكم بالمعلومات التي تراها على شاشة حاسبك. في عالم تمثل فيه المعلومات القوة، يمكن للسدنة الذين يتحكمون بتدفق البيانات التي تصل إلى شاشتك أن يتحكموا بغيرها. وهو سلوك نواجهه كل يوم في كل مرة ندخل فيها إلى الإنترنت. فمعظمنا لا يقرر القيام بعملية شراء أو بحجز طاولة في مطعم جديد لإحياء مناسبة خاصة، دون القيام أولاً ببحثٍ على الإنترنت. فمن يستطيع إطلاعنا على ما نريد أفضل ممن سبقونا إلى التسوق وتناول العشاء؟ يقول حوالى 90 بالمئة من المستهلكين إن استعراض الإنترنت يؤثر في قراراتهم المتعلقة بالشراء، وقد وجدت دراسة لنيلسن أن نسبة مفاجئة تقدر بحوالى 70 بالمئة من الناس يثقون بمراجعات المنتجات التي يقرأونها على الإنترنت أكثر مما يثقون بنصائح أصدقائهم. لكن لسوء الحظ فإن 25 بالمئة من المراجعات التي تمت على موقع ييلب، وهو من أشهر المواقع من هذا النوع، هي مراجعات ملفقة تماماً وفقاً لتحقيق أُجري من قبل النائب العام لولاية نيويورك. والأسوأ من ذلك بعد أن محكمة الاستئناف الفدرالية حكمت في أيلول عام 2014، بأنه من القانوني بالنسبة لموقع ييلب التلاعب بمستوى تصنيفاته معتمداً على الشركات المُعْلِنة على الموقع؛ أي إن بإمكان المنفقين الكبار الحصول على خمس نجوم وبشكلٍ قانوني، حتّى لو منحهم جميع المستخدمين نجمة واحدة فقط. ومراجعات مواقع إيباي وأمازون وتريب أدفايسور، كلها يمكن تلفيقها بسهولة أيضاً، وكثير من تصنيفات الخمس نجوم التي تراها هناك كانت تكتبها الشركات نفسها أو تكلف بها عملاء مأجورين. هنالك أيضاً شركات محترفة يقوم نموذجها التجاري برمته على التلاعب بنظام مراجعات الإنترنت. وتُعرف هذه المؤازرة باسم التنجيم وهي واسعة الانتشار. وقد حققت ولاية نيويورك في أمر إحدى هذه الشركات واسمها

زامديل إنك.، كانت قد اتُّهمت بتدوين ألف وخمسمئة مراجعة مزيفة على الأقل على مواقع ييلب وغوغل للأماكن.

كنت أظنك صديقي

وفقاً لتقرير فايسبوك السنوي الصادر عام 2014، فإن أكثر من 11.2 بالمئة من حساباته مزيفة. إذا أخذنا في الاعتبار عدد المستخدمين في أضخم شركة للتواصل الاجتماعي في العالم، والبالغ عددهم 1.3 مليار مستخدم، فإن ذلك يعني أن أكثر من 140 مليون حساب على الفايسبوك هي حسابات مخترعة وأن هؤلاء المستخدمين ببساطة غير موجودين. مع 140 مليون نسمة، ستكون أرض الفايسبوك الزائفة هذه عاشر أكبر بلد في العالم. تماماً كما حددت تصنيفات نيلسن على أجهزة التلفاز معدلات إعلان لفيلم الأموات الأحياء تختلف عن تلك التي تضعها لبطولة لعبة البولينغ، تُحدد مبيعات الإعلانات على الإنترنت بمقدار ما يمكن لكل موقع أو خدمة اجتماعية الحصول عليه من مشاهدات.

هل تريد أن يكون لديك 4000 متتبع على تويتر؟ لك ذلك مقابل خمسة دولارات. وهل تريد أن يكون لديك 100000 مُعْجب على فايسبوك؟ لا مشكلة في ذلك، يمكن أن تشتريهم من موقع SocialMediaCorp.org مقابل 1500 دولار فقط. هل لديك الكثير من المال لتنفقه؟ ما رأيك بمليون صديق جديد على إنستاغرام؟ "لأجلك نقدم صفقة خاصة"، 3700 دولار فقط. إذا كنت تريد الأشياء المفضلة أو الإعجابات أو إعادة التغريدات أو التصويت أو معاينة الصفحات، فكل ذلك متوفر للبيع على مواقع مثل سوينزي وفيفر وكرايغسليست. تُستخدم هذه الحسابات المخادعة لمنح دعم مزيف لمنتج أو خدمة أو شركة مقابل رسم بسيطٍ طبعاً. ويتم إنجاز القسم الأكبر من العمل في العالم النامي، مثل الهند وبنغلادش، حيث

يتحكم ناس حقيقيون بهذه الحسابات. أما في أماكن أخرى، مثل روسيا وأوكرانيا ورومانيا، فيتم إنجاز العملية بشكلٍ كامل من قبل روبوتات برمجية، وهي برامج بسيطة تنفذ تعليماتك المؤتمتة المبرمجة، مثل "انقر على زر الإعجاب"، مراراً وتكراراً باستخدام شخصيات مزيفة مختلفة.

تماماً مثل المخلوقات المتحولة الأسطورية التي كانت قادرة على التحول مادياً من كائن إلى آخر، كذلك تتمتع المخلوقات المتحولة المعاصرة التي تظهر على الشاشات بقواها السحرية، والمجرمون تواقون لتجريبها، فهم يقومون بدراسة تقنياتها وتوظيفها ضد أهدافٍ سهلة لتحقيق أرباح ضخمة. وكثير من نقرات الفأرة التي تشهدها الشاشات إنما هدفها "الاحتيال بالنقرات". فالشركات تدفع المال لشركات الفايسبوك وغوغل لقاء كل نقرة يقوم بها زبون محتمل على أحد أشرطة الإعلانات أو الروابط التي تراها على الإنترنت، لكن عصابات الجريمة المنظمة وجدت طرقاً لاستغلال هذا النظام بحيث تحقق أرباحاً بطرقها الخاصة عبر ما يُعرف بشبكات الإعلان، التي تجعل بدورها من تلك النقرات الإضافية رأسمال لها. لكن بعد تصاعد الانتقادات، حاولت شركات التواصل الاجتماعي أن تقلل عدد الحسابات الزائفة. فكانت نتائج إجراءات الفايسبوك واضحة. حيث خسرت كل من ريهانا وشاكيرا 22000 معجب على الفايسبوك، وكذلك ليدي غاغا التي ألغي 32000 من معجبيها، وأيضاً لعبة Texas Hold 'Em Poker من شركة زينغا التي تبخر 100000 من مشجعيها المزعومين.

إذا كان لدى الفايسبوك 140 مليون حساب زائف، فلا بد من أن هذه الحسابات قد أُنْشِئت يدوياً الواحد تلو الآخر، ولا بد من وجود شيء أكثر خبثاً بكثير وراء هذا العمل، وهذا الشيء موجود بالفعل. يُسمّى هذا العمل بجورب العرائس، وهو إشارة إلى لعبة الأطفال التي يتم صنعها

عندما توضع اليد داخل الجورب لخلق شخصية حيّة. ففي عالم الإنترنت، تقوم عصابات الجريمة المنظمة بخلق تلك العرائس عن طريق الجمع بين البرمجة الخطاطية وأتمتة الشبكات ومواقع التواصل الاجتماعي، لتحصل على جيوشٍ من الشخصيات على الإنترنت. ويمكن أن يتم ذلك بسهولة وبكلفة زهيدة تسمح لسيئي النوايا بفبركة مئات الآلاف من المواطنين على الإنترنت.

ما على المرء سوى مراجعة دليل الأسماء الشائعة المتوفر على الإنترنت لأي بلد أو منطقة. فيمكنك أن تجعل برنامجك التخطيطي ينتقي الاسم الأول والكنية ويختار تاريخ الميلاد، وينشئ حساب بريد إلكتروني مجاني. بعد ذلك، يمكنك الدخول إلى أحد مواقع الصور مثل بيكاسا أو إنستاغرام أو فايسبوك أو غوغل أو فليكر لتختار الصورة المناسبة التي ستمثل دميتك الجديدة. مسلحاً بتلك التفاصيل، مثل عنوان البريد الإلكتروني والاسم وتاريخ الميلاد والصورة، لا يبقى عليك سوى التسجيل في حسابٍ على الفايسبوك أو تويتر أو إنستاغرام. أما الخطوة الأخيرة فهي تعليم الدمى الكلام عن طريق تلقينها كيفية التواصل وإرسال طلبات الصداقة وإعادة كتابة تغريدات الناس الآخرين، والإعراب بشكلٍ عشوائي عن إعجابها بالأشياء التي تراها على الإنترنت. ويمكن لبرامجك أيضاً أن تتصل وتتبادل المدونات في ما بينها. وقبل أن تلاحظ ذلك، سيكون لديك آلاف العرائس تحت تصرفك تستخدمها كما يحلو لك. يستخدم المجرمون هذه الجيوش من الدمى كعناصر أساسية في عمليات التصيّد الإلكتروني وفي تزييف مراجعات الإنترنت ولاستدراج المستخدمين لتحميل برمجيات التجسس، وفي تنفيذ مختلف عمليات الاحتيال المالية.

خطأ النظام القاتل

إننا نعيش الآن في عالم "الإيمان بالشاشة". فنحن نلجأ في المقام الأول إلى

الحواسب للحصول على الإرشاد والتوجيه، ونعتمد على الشاشات للحصول على الأجوبة، ونادراً جداً ما نشك بالنتائج. لكن إذا كانت البرمجة ضعيفة أو البيانات الأساسية خطأً، فسوف تنعكس هذه الأخطاء على النتائج التي تحصل عليها. فمن البديهيات الأساسية في علم الحاسب أن رداءة المعلومات المدخلة إلى الحاسب تقود إلى معلومات خارجة رديئة. كان اعتمادنا المحدود على التكنولوجيا في الماضي هو ما يعزلنا ويحمينا من مثل هذه الأخطاء. أما في عصر البيانات الكبيرة، فقد تغيرت جميع الحسابات. فجميعنا يتأثر بأخطاء قواعد البيانات بطريقةٍ أو بأخرى، ولا تنفكّ تزداد تبعات هذه الأخطاء يوماً بعد يوم. فوفقاً لوكالة التجارة الفدرالية، يعاني حوالى 25 بالمئة من تقارير أرصدة المستهلكين من وجود أخطاء، وقد اعترف بعض سماسرة البيانات، مثل أكسيوم، بأن 30 بالمئة من البيانات التي يجمعونها ويحتفظون لها قد تكون غير دقيقة.

عندما يتأثر أربعون إلى خمسين مليون أميركي بهذه الأخطاء لدى استئجار شقة أو شراء سيارة أو الحصول على رهن أو التقدم إلى وظيفة، فإنهم سيكتشفون عما قريب أن خطأ شخصٍ آخر أصبح الآن كابوساً يعيشونه. فإذا كان منحك قرضاً يعتبر مجازفة "وفقاً لحاسبنا"، فلا يوجد لديك أية أعذار. وملايين القرارات يتم اليوم اتخاذها باستخدام بيانات زائفة وناقصة وغير دقيقة، وغالباً دون التحقق من صحتها. ولو كانت المشكلة مقتصرة على التقارير المصرفية لكان من الممكن التغاضي عنها. لكن العيش في أرض "الإيمان بالشاشات" يعني أن الأخطاء الحاسوبية يمكن أن تؤثر على حياتنا وحريتنا لا فقط على مواردنا المالية.

فيما يندفع عالم الطب نحو رقمنة سجلات المرضى في محاولةٍ لتوفير المال وتحسين الكفاءة وتطبيق الرؤى الجديدة للبيانات الكبيرة على الحالات المرضية، ثمة ضحية لم تكن متوقعة هي الدقة. إذ تحتوي عشرات ملايين

السجلات الطبية الإلكترونية على معلومات خطأ عن المرضى، ويمكن لمثل هذه البيانات الخطأ حين تظهر على الشاشة أن تكون قاتلة بكل ما في الكلمة من معنى. فقد توفّي غاري فوستير، البالغ من العمر سبعة وعشرين عاماً من مدينة إسيكس في إنكلترا، في مشفى الجامعة في لندن عندما أشار خطأ في نظام حاسب المستشفى إلى أن الشاب تلقى جرعة زائدة من أدوية السرطان أثناء إقامته في المشفى. حيث قام الفريق الطبي، الذي اتبع الخطة الطبية المدخلة عن طريق الخطأ، بتزويد المريض بجرعات قاتلة من المواد الكيميائية لعلاج سرطان الخصيتين. إن ثقتنا الزائدة بشاشات حواسبنا لا يمكنها أن تسبب القتل فحسب، بل يمكن لها أيضاً أن تترك أثراً ضاراً على السلامة العامة.

وفي ولاية كاليفورنيا، أدى خلل في الحاسب إلى تحرير 450 مجرماً خطيراً بعد أن وجه أمرٌ خطأ في النظام لحراس السجن بإطلاق سراح عددٍ من المجرمين الأكثر خطورة في الولاية. وكان من بين هؤلاء أعضاء عصابات ومغتصبون ولصوص مسلحون وسجناء مصنفون على "أعلى درجات الخطورة المتعلقة بالعنف"، خرجوا جميعاً من سجون في كافة أرجاء الولاية لأن موظفي السجن صدقوا المعلومات التي شاهدوها على شاشات حواسبهم. والأخطاء في بيانات العدالة الجنائية هي أمرٌ شائع بالطبع، وهي لا تحرر المتهم فقط، بل تتهم البريء أيضاً. ففي بريطانيا، اعترف ضباط الشرطة في دائرة السجلات الجنائية المحلية بأن أكثر من عشرين ألف شخص تم اعتبارهم خطأً مجرمين بسبب أخطاءٍ في بيانات تلك الأنظمة. وهي أخطاء بالجملة تعني أن الآلاف من الأبرياء قد فُتحت لهم سجلات جنائية على جرائم لم يرتكبوها أبداً. "لكنك يا سيدي أمسكت بالشخص الخطأ" هي عبارة اعتاد ضباط الشرطة سماعها؛ لكن لسوء حظ أولئك المتهمين، ما هو موجود على الشاشة هو الصحيح، حتى يثبت العكس. فقد

كان ضحايا هذه الأخطاء يحرمون من فرص العمل وإمكانيات التطوع في أنحاء المملكة المتحدة وتتعرض سمعتهم للأذية، وكل ذلك بسبب إيماننا الراسخ بشاشاتنا.

إننا نواجه اليوم حشداً من الظواهر، البشرية والتقنية، اجتمعت معاً كالعاصفة الهوجاء لتخلق مخاطر هائلة تتهدد مجتمعنا. ومع كل جيل جديد، نزداد اعتياداً، ولو لم ندرِ، على الاتباع الأعمى للتوجيهات الصادرة لنا عن الآلات. البديهية التي ذكرناها سابقاً في علم الحواسب، والتي تقضي بأن رداءة المعلومات الداخلة إلى الحاسب تؤدي إلى رداءة في المعلومات الخارجة منه، حلت محلها بديهية جديدة تقضي بأن كل ما يصدر عن الحاسب هو مقدس: إذا كان هذا ما يقوله الحاسوب، فلا بد أنه محق فيه. المشكلة في هذا التفكير هو أننا كمجتمع نعتمد كل الاعتماد على بيانات خطأ طوال الوقت، وهي مشكلة مزمنة ستعود آثارها السلبية علينا. ففقاعات الفلاتر، والرقابة الخفية لمحركات البحث، وجدران النار الوطنية، والبيانات الخطأ، كلها تشير إلى أننا نعاني مشكلة أساسية في تصورنا للعالم، أو، لمزيد من الدقة، في الطريقة التي يتم من خلالها تقديم العالم إلينا عبر وساطة شاشاتنا.

الرؤية لا تعني التصديق

ركزنا في الفصول السابقة من هذا الكتاب بشكلٍ كبير على ما يحدث عندما يتم تسريب بياناتك واختراق خصوصية معلوماتك. وما من شك في أن لدى المجرمين القدرة على المناورة مع كافة الفرص التي يخلقونها من خلال سرقة بياناتك. لكنْ هنالك تهديد أكثر عمقاً وغدراً لمعلومات العالم، وهو تغيير هذه المعلومات. إذ يقوم المجرمون والقراصنة والإرهابيون والحكومات باقتحام أنظمة البيانات، ليس بهدف سرقة المعلومات، بل بهدف التلاعب خلسة بطريقة عرضها على شاشاتنا، كما رأينا في حادثة

منشأة ناتانز. أي إن نزاهة معلومات العالم هي هدف الهجوم. برويّة وسرية ودقة عالية، يدخل المهاجمون إلى أنظمة بياناتنا ويغيّرون سرًّا كافة المعلومات فيها. فهجوم القراصنة بهدف سرقة بياناتنا ربما كان أفضل السيناريوهات إذا ما قورن بتغيير المعلومات دون علمنا.

عام 1995 أدت ساندرا بولوك في فيلم الشبكة، دور محللة أنظمة مستقلة تقوم بالصدفة باكتشاف مؤامرة تحوكها منظمة إرهابية سايبرية للاستيلاء على أنظمة معلومات العالم. ويبدأ الفيلم بمشهدٍ يقوم فيه وكيل وزارة الدفاع بالإقدام على الانتحار بعد علمه بأن التحاليل التي أجريت له في مشفى بيثيسدا نافال قد بينت أنه يحمل فيروس الإيدز، ليتبين في ما بعد أن الضابط لم يكن يحمل فيروس الإيدز، بل كان القراصنة قد عدلوا نتائج الفحوصات الطبية انتقاماً منه بسبب ملاحقته للأشرار الإلكترونيين العالميين. وقد قام طبيبه بنقل هذه المعلومات بأمانة معتمداً على البيانات الظاهرة على شاشة حاسبه. كان الإحراج الذي سببته نتائج الفحوصات للوكيل المُحافظ كبيراً إلى حد دفعه إلى الانتحار.

هذا هو عالم حرب المعلومات الذي تنتشر فيه المعلومات الحاسوبية الخطأ عبر مختلف الشاشات التي تومض فارضةً تأثيرها على العالم الحقيقي. من الممكن جداً للأحداث التي صُوّرت في الفيلم أن تحدث على أرض الواقع اليوم. إذ يتم اختراق أنظمة بيانات الشرطة في كافة أنحاء العالم، كأستراليا وإنكلترا وإيطاليا وممفيس ومونتريال وهونغ كونغ وهونولولو. فعام 2013، تم اختراق مكتب منح رخص القيادة التابع للشرطة الدانمركية، واعتُقِد أن القراصنة قاموا بتغير أنظمة البيانات الخاصة بالسلطة التنفيذية. وفي ولاية فيلادلفيا الأميركية كذلك. وفي العام نفسه، قامت عصابة إجرامية محلية باختراق قاعدة بيانات سرية خاصة بشهادات تتعلق بأشهر الجرائم في المدينة. ونتيجة لهذا العمل، تم وضع أسماء

وعناوين وصور العشرات من الشهود المحميين على موقع إنستاغرام تحت العنوان الفرعي "فضح الجرذان". وكان كثير من هؤلاء الأفراد المفضوحين قد أدلوا بشهاداتهم أمام جلساتٍ سرية لهيئة المحلفين، ولم تكن سوى بضعة أيام حتى صار هنالك حوالى ثمانية آلاف متتبع لحساب الإنستاغرام المعروف باسم الجرذان 215. وقد تعرض في ما بعد أحد الشهود في التاسعة عشرة من عمره، كان قد أدلى بشهادته في قضية قتل، لإطلاق نار في عملية انتقامية. وفيما لا يعتبر ترويعاً للشهود بالجملة، قام العديد من زائري الموقع بوضع تعليقات متنوعة مثل "اقضوا على الجرذان" و"اضربوهم أينما وُجدوا".

وفي ولاية ماساتشوستس، سُمح لسجين محكوم بقضية قرصنة بالدخول إلى مكتبة السجن للقيام ببحث قانوني يخص قضيته. وما إن لامست أصابعه لوحة المفاتيح، حتى تمكن من الدخول إلى شبكة حاسب قسم إعادة التأهيل والحصول على ملفات قضايا السجناء الآخرين، بالإضافة إلى الحصول على أسماء حراس السجن الأحد عشر ألفاً وتواريخ ميلادهم وأرقام ضمانهم الاجتماعي وعناوين منازلهم وأرقام هواتفهم. إذا ما أخذنا بالاعتبار هذا النقص في أمن أنظمة العدالة الجنائية، فكم يبلغ عدد المساجين الذين أُطلق سراحهم بالخطأ، كما حدث مع 450 مجرماً خطيراً في كاليفورنيا، بسبب تزييف البيانات والتلاعب بها؟ الجواب ببساطة، هو أننا لا نعرف، وهي مسألة يكره موظفو الحكومة الخوض فيها.

بالرغم من انفتاح وضعف حواسب السلطة التنفيذية، إلا أنها أشبه بحصن كنوكس إذا ما قورنت بسجلاتنا الطبية الإلكترونية. وبغض النظر عن ملايين الأخطاء العابرة التي أشرنا إليها في السابق، فقد أشار قسم الصحة والخدمات الإنسانية إلى أن حوالى واحد وعشرين مليون أميركي تم الدخول إلى سجلاتهم الطبية الإلكترونية دون إذنٍ منذ عام 2009. بل إن القسم قد

وثق أكثر من تسعمئة حالة اختراق في المشافي الموجودة في الولايات المتحدة الأميركية. لكن ماذا عن الحالات العديدة التي لم تتم الإشارة إليها؟ ينص القانون الفدرالي بإعداد التقارير إذا كان الاستهداف يشمل أكثر من خمسمئة سجل لكل حادثة على الأقل. ويستهدف المجرمون المنظمون البيانات الطبية بطرق عديدة ومتنوعة، تتراوح بين تزوير نظام المساعدة الطبية للمسنين والابتزاز. ففي ولاية فرجينيا، قام القراصنة بالدخول إلى سجلات ثمانية ملايين مريض ووصلوا إلى خمسة وثلاثين مليون وصفة طبية محفوظة لدى قسم الصحة، وهدّدوا بنشر المعلومات على الإنترنت إذا لم تدفع لهم الولاية فدية قيمتها 10 ملايين دولار. أما عالمياً، فتعاني أنظمة البيانات الطبية نقاط ضعف جوهرية، تسمح للمجرمين باستغلال هذه البيانات كما يريدون، ما يقود إلى عواقب وخيمة.

مراراً وتكراراً، سيتبع الأطباء والممرضات والفنيون توجيهات شاشات الحواسب التي تعرض عليهم، حتى عندما تكون المعلومات خطأً، كما رأينا سابقاً عندما وصفنا الأخطاء القاتلة لنظام المستشفى الذي أدى إلى وفاة غاري فوستير. فحين تقرر الشاشة أنك تحمل فيروس الإيدز، سيقوم أطباء المستشفى بإعلامك بهذه النتائج. والأسوأ من ذلك بعد أنه إذا أظهرت التحاليل أن زمرة دمك هي O إيجابي وقام قرصان أو خصم لك بتغييرها إلى A سلبي في قاعدة بيانات المستشفى قبل دخولك إلى العملية الجراحية، فإن نتيجة العملية الحتمية هي الموت. وقد هو ما سيكون أيضاً إذا قام شخص حاقد بإزالة حساسيتك للبنسلين من بياناتك الرقمية لتقوم الممرضة من دون علم بتنفيذ الأمر الطبي الموجه إليها بحقن خمسمئة مليغرام من هذا العقار في أوردتك.

يمكن للعواقب الكبيرة المرتبطة بطريقة التفكير القائمة على الثقة بالشاشات أن تفتح الباب أمام سلسلة من الجرائم الجديدة، من ضمنها

طرق جديدة للقتل. وقد قام المجرمون بتطوير ترسانة من الأساليب التي تسمح لهم باستغلال عالمٍ سخّر الذكاء البشري لمصلحة العالم الرقمي والافتراضي. والمجرمون يبدون مهارة في ما يُسمى هجمات الوسيط، حيث يُقحمون أنفسهم بين الواقع وبين البيانات التي نشاهدها على شاشاتنا. أما النتيجة، فهي اعتداء سافر على صحة المعلومات التي نكدسها في سياق ثورة البيانات الكبيرة.

شاشة الجريمة

طوّر المجرمون خطة هجوم خاصة لكل شاشة في حياتك. وإحدى أشهر هذه الحيل على الإنترنت هي ظاهرة التصيّد، وهي تقنية يقوم من خلالها المجرمون بالتنكر بهيئة موقع إلكتروني قانوني لكي يحصلوا على معلومات مثل كلمات السر وأرقام بطاقات الائتمان. ومصطلح "التصيّد (phishing)" هو تحريف خرج به القراصنة لكلمة "اصطياد (fishing)"، وتقوم هذه التقنية على إغراء سمكةٍ بريئة بابتلاع طعم هو عبارة عن رابط خبيث. وتحاول عصابات الجريمة المنظمة التي تقود عمليات التصيّد أن تحتال على المستخدمين بجعلهم ينقرون على رابط يأخذهم إلى موقع إلكتروني زائف يُدار من قبل المخادعين أنفسهم. إذ تصل رسائل الخداع إلى صندوق رسائلنا الواردة أو تأتينا على شكل رسائل قصيرة وتغريدات ورسائل فورية وتحديثات حالات على الفايسبوك. ويكون المصدر المزعوم لهذه الرسائل هو البنوك أو شركات الاتصال أو برامج التقاعد أو منافذ التواصل الاجتماعي أو خدمات الهواتف النقالة. وتستهدف هذه الهجمات المستخدمين في شتى أنحاء العالم، وإن كان العدد الأكبر من ضحاياها في الولايات المتحدة الأميركية والمملكة المتحدة وألمانيا.

وفي النهاية، تعتمد كافة هجمات التصيّد على وجود مستخدم غافل يقوم بالنقر على الرابط أو الملف الملحق بالرسالة، فإما أن تقود الرسالة الضحية

إلى موقعٍ إلكتروني احتيالي أو يتم تنصيب برمجية خبيثة على جهازه. ويستغل المجرمون الروابط الفائقة على صفحات HTML حيث يبيتون فيها تعليمات الهجوم ضمن تعليمات الحاسب المخفية. وتصلنا رسائل التصيد على شكل بطاقات إلكترونية مزيفة أو بريد إلكتروني من مصرفنا أو كعروض العمل أو قسائم أو صفقات لا يمكن أن تكون حقيقية على مواقع التواصل الاجتماعي. هذه البلاغات الشريرة، التي كانت تعج بالأخطاء النحوية والهجائية في السنوات السابقة، أصبحت اليوم احترافية يتعذر عملياً تمييزها عن الرسائل الحقيقية. ويعرف المجرمون تماماً كيف يستغلون الثقة التي وضعتها بالشاشات عبر المحاكاة البصرية للمواقع التي ينتحلون هويتها وخداع أحاسيسك بمسحة يد رقمية.

قد تصلك رسالة اعتيادية من عنوانٍ مثل securi، تخبرك بضرورة تحديث حسابك أو بأن حسابك معطّل نتيجة نشاط مريب. فتقول لنفسك إن الأمر يبدو مهماً، ومن الأفضل الاطلاع عليه. لكن ما لا تدركه هو أن البريد الإلكتروني الذي ظهر في صندوق الرسائل الواردة إليك من السهل محاكاته أو تزويره. ففي كل مرةٍ تقوم فيها بإنشاء حساب بريدي جديد على أي برنامج مثل آوتلوك أو ماك.ميل أو ثاندربيرد، سوف يُطلب منك إدخال الاسم وعنوان البريد الإلكتروني. وإذا قام المحتال بتسجيل عبارة مثل "الفريق الأمني لبنك أميركا" كاسمٍ في برنامج البريد الإلكتروني، فهذا ما سيظهر في صندوق الوارد لديك. الأمر بهذه البساطة. فقط بالتدقيق في ترويسات الرسالة الداخلية، قد تلاحظ أن عنوان البريد الإلكتروني المستخدم من قبل أولئك الأشخاص السيئين كان في الواقع notifications@security-bankofamerica.com، وهو قريب من عنوان البريد الإلكتروني الأصيل بما فيه الكفاية لخداع شخصٍ عادي.

تبدو الرسالة، كيفما نظرت إليها، وكأنها صادرة عن المصرف الذي تتعامل

معه، ففيها نمط الخط نفسه واللون والشعار ذاتهما، لكنها في الواقع مزيفة. فبالرغم من أن الرابط الظاهر قد يكون ،، فإنه سيوجهك عوضاً عن ذلك إلى www.bank0famerica.com (الرقم 0 بدلاً من الحرف o) أو حتّى bankofamerica.accountupdates.com (بينما سيكون النطاق الفعلي الذي ستزوره هو accountupdates.com الذي تعود ملكيته للمجرمين؛ وBank of America هو مجرد ملف أعدوه في موقعهم لخداعك)؛ وكذلك موقع www.citibank.com سوف يحل محله www.citiibank.com (هنالك حرفا i في الموقع الزائف بالكاد يمكن ملاحظتهما). تصرخ رسائل التصيد على نحو ملتبس بما تريد منك فعله، بحيث تجعل من المستحيل تجاهل الرابط الذي دست في حبة السم، إذ يُكتب الرابط بخط كبير واضح أو يزوّد بزر كبير ملون: "لتحديث إعدادات الحماية ووقاية حسابك، انقر هنا". وبهذا يسيطرون عليك.

ستقودك هذه النقرة المميتة إلى موقع Citiibank.com، حيث سيطلب منك تسجيل الدخول عبر إدخال بيانات المستخدم، وعندما تقوم بذلك، يستولي اللصوص على اسم المستخدم وكلمة السر بالإضافة إلى باقة من المعلومات الشخصية الأخرى. وفي هذه اللحظة بالذات يكون قد حان وقت العمل بالنسبة للمجرمين. فما التصيد سوى جريمة عبور، وهو الخطوة الأولى والأساسية التي تزود اللصوص بالبيانات الضرورية لإنجاز الخطوة الثانية في المكيدة التي حاكوها ضدك، والتي تتضمن سرقة الهوية والاحتيال المالي والضريبي والتأميني. وتماماً كما تم تقديم واقع مقنع، لكنه ملفق تماماً، على شاشات المهندسين النوويين في منشأة ناتانز، ستتعرض بدورك للهجوم من قبل المجرمين الذي يقرعون على بابك كل يوم.

إن تكاليف إنجاز هذه التمثيليات الرقمية بالنسبة للمجرمين منخفضة إلى حدّ التفاهة. ففي الأوساط الرقمية السرية، تباع معدات الاحتيال

المؤتمتة اللازمة لإرسال رسائل تصيّد لخمسمئة ألف بريد إلكتروني بتكلفة لا تتجاوز الـ 65 دولاراً. وكما ذُكر سابقاً، يستفيد المجرمون من حسابات "جورب الدمى" لتوسيع عملياتهم. وهو ما يفسر وصول أكثر من 100 مليون رسالة تصيّد إلى صندوق رسائلنا الواردة في كل يوم. تشير دراسة أجريت من قبل سيسكو تناولت الجوانب الاقتصادية لهذه الهجمات، إلى أن حوالى ثمانية أشخاص من أصل مليون ستنطلي عليهم الخدعة بمعدل خسارة يصل إلى 2000 دولار لكل ضحية. أي إن بإمكان اللصوص أن يجنوا 1 دولار مقابل 130 دولاراً، بنسبة 12000 بالمئة تعود للاستثمار. وبوجود 36 مليار رسالة تصيّد تُرسلْ سنوياً، تزداد الجرائم الإلكترونية توسعاً وربحية. وعلى الرغم من أن عائدات هجمات التصيّد الضخمة مميزة، إلا أنها تصبح باهتة إذا ما قورنت بـ "تصيّد الحربة"، وهي تقنية لا تعتمد على إرسال رسائل تصيد إلى الملايين من الناس، بل تستهدف، خلافاً لذلك، بتأنّ أشخاصاً محددين أو منظماتٍ بعينها.

أصبح تصيّد الحربة هو الاختيار المفضل لدى أولئك الذين يؤازرون التجسس الصناعي، والتكاليف في هذه الحالات ضخمة، كما اكتشفت شركة كوكا كولا العملاقة للمشروبات الغازية. كجزءٍ من عمليات توسعها في آسيا، دخلت شركة كوكا كولا في مفاوضات متقدمة لشراء مجموعة شركات هيووان جويس الصينية. وكان كل شيء يسير حسب الخطة المرسومة لإتمام عملية الشراء، إلى أن فشلت الخطة بشكلٍ غامض. كان ثمة شيء مبهم في مجريات الأحداث، وكانت شركة كوكا كولا تبحث عن تفسير. وكان أن أجرت الشركة تحقيقاً شاملاً في القضية، فبدأت بمراجعة الصفقة بالتفصيل، واشتملت المراجعات على الاتصالات المجراة بين كوكا كولا وممثلي مجموعة هيووان جويس. وفي النهاية، اكتشفت شركة كوكا كولا أن الحكومة الصينية كانت قد أقحمت نفسها عبر مراقبة الصفقة وأنها كانت تتابع سراً خطط

شركة كوكا كولا ونواياها في إطار عملية المزايدة. لكن كيف حصل الصينيون أساساً على إمكانية الدخول التي يحتاجون إليها؟ لقد كان لهم ذلك عن طريق التلاعب بشاشة بول إيتشيلز، نائب رئيس مجموعة شركات كوكا كولا باسيفيك.

كان إيتشيلز قد فتح رسالة بريد إلكتروني مُقلّد، بدا وكأنه مرسل من موظفٍ أعلى مركزاً منه في القسم القانوني لكوكا كولا. وكان العنوان الرئيسي للبريد الإلكتروني مغرياً: "وفر الطاقة، وفر النقود، من المدير التنفيذي لشركة كوكا كولا". كان إيتشيلز يعلم أن مديره في الشركة كان يناضل بقوة في سبيل توفير الطاقة في الشركة (كما كان الصينيون يعلمون بذلك أيضاً بعدما قاموا بالتسلل إلى أنظمة المعلومات التجارية لشركة كوكا كولا). قام منفذو الهجوم بتقليد الحقيقة عبر جعل الرسالة تبدو وكأنها مُرسلة من زميل موثوق في العمل، على الشبكة الداخلية للشركة، ومع عنوانٍ رئيسي مقنع منسجم مع سياقه. فعندما قام نائب رئيس شركة كوكا كولا بكل براءة بالنقر على الرابط، تم تحميل برمجية خبيثة على الحاسب الذي يستخدمه خلسة، وكانت البرمجية قادرة على التقاط جميع المفاتيح التي يضغطها الموظف. نتيجة لذلك، صار بإمكان الصينيين تنزيل مخزون كبير من ملفات الحاسب المرتبطة بالصفقة. وبينما رفضت شركة كوكا كولا التعليق علانية على هذه "المسألة الأمنية"، كان واضحاً أن هجوماً واحداً من هجومات "التصيّد بالحربة" استهدف موظفاً رفيع المستوى في شركة كوكا كولا قد كلف الشركة قيمة استحواذها على مجموعة هيووان جويس الصينية، التي كانت تبلغ 2.4 مليار دولار. ليست شركة كوكا كولا وحدها التي تعرضت للتصيد بالحربة، فقد باتت هذه الظاهرة هي الأداة التكتيكية المفضلة لدى مجرمي الإنترنت والجواسيس الرقميين المسؤولين عن 91 بالمئة من الهجمات السايبرية.

يمكن للمجرمين أيضاً تغيير ما تشاهده على شاشتك بالزمن الحقيقي، بما في ذلك حساباتك المالية. فماذا لو كان رصيد حسابك في البنك منتهياً، ولم تكن تعلم بذلك؟ ثمة هذه الأيام الآلاف من برامج البرمجيات الخبيثة القادرة على سرقة النقود من حسابك المصرفي، وقد أصبحت العملية برمتها روتينية، بل ومؤتمتة أيضاً. يصيب المجرمون حاسبك أو هاتفك النقال بفيروس، ويحصلون على المعلومات المُعْتَمدة للدخول إلى حساباتك، ومن ثم يستخدمونها لاستنزاف رصيدك المصرفي. ومن الممكن بالطبع أن يحدث أن تدخل بنفسك ذات مرة إلى حسابك لتلاحظ انخفاض رصيدك، وستقوم عندها بإبلاغ قسم مكافحة الاحتيال في البنك لتُوقف تحويل الأموال. فعادة ما تقوم البنوك بإبقاء فترات إنجاز عمليات تحويل الأموال، وخاصة الدولية منها، مفتوحة ليوم واحد على الأقل بحيث يمكنها إلغاء عملية تحويل أو إرسال الأموال أو إيقافها أو عكسها، ما يجعل مجال التلاعب ضيقاً للغاية. لذا، فإن المجرمين يبذلون قُصارى جهدهم لضمان أن ما تشاهده على شاشة حاسبك ليس هو ما تملكه في حسابك المصرفي. فثمة برمجيات خبيثة أحصنة طروادة عالية التخصص، مثل SpyEye وURLZone، لا تسرق نقودك فحسب، بل تقدم لك تطمينات زائفة بأن النقود لا تزال في حسابك المصرفي. يكمن سحر هذه البرامج في أنها تمنح اللصوص الوقت الكافي لاستخدام المعلومات المتعلقة بحسابك المصرفي ومناقلاته المدينة وببطاقتك الائتمانية دون علمٍ منك. ولن تعلم بوجود مشكلة سوى عندما تحاول استخدام بطاقتك المصرفية لسحب الأموال لتعلم عندها أنك تجاوزت الحد المسموح للسحب وأنه ما من رصيد كافٍ في الحساب.

إن البرامج الإجرامية المُسْتخدمة متطورة جداً، إلى حد أنها تعرف قدر الأموال المسروقة من كل حسابٍ مصرفي قامت باختراقه. أي إنه عندما

يسرق اللصوص 2419 دولاراً من حسابك، ستقوم الخوارزمية بإضافة هذا المبلغ إلى الرصيد الذي يظهر على شاشتك بالزمن الحقيقي عندما تتفقد رصيد حسابك عبر الإنترنت. أما عمليات الشراء التي يُجريها المجرمون بواسطة بطاقتك الائتمانية أو بطاقتك المدينة فيتم استبعادها تلقائياً من قائمة المناقلات السابقة ومن كشف الحساب الموجود على الإنترنت، قبل أن تظهر على شاشتك. وحتى ملفات بي.دي.إف التي تحوي المناقلات المصرفية، والمُرسلة إلى طابعتك، يتم تعديلها قبل خروجها من آلتك. عندما يريد اللصوص السيطرة عليك فإنهم يستطيعون ذلك حقاً.

يذكّر هذا النوع من الهجمات المعتمدة على وسيط بأن القراصنة المجرمين قادرون تماماً على التوسط بينك وبين واقعك بفضل هذا الكم من الشاشات المتزايد أبداً في حياتك. فتماماً مثل دودة ستوكسنيت، يدرك هؤلاء المجرمون أن الشاشات هي مجرد تمثيل للواقع، تمثيلٍ طيّع يسهل التلاعب به. إلا أنه لا تتم جميع عمليات التلاعب بالبيانات التي نراها على شاشاتنا على يد عصابات جريمة سايبرية أو عن طريق خدمات التجسس.

فعادةً ما يتقمص البيدوفيليون شخصيات رقمية لأطفال، ويعجز غير البالغين في 80 بالمئة من الحالات عن اكتشاف أنهم يتحدثون مع شخص بالغ، ما يجعل شاشات اليافعين عرضة للهجوم على نحو خاص. ولنتذكر قضية أماندا تود، الفتاة البالغة من العمر اثني عشر عاماً التي تم خداعها لتعرض صدرها على الكاميرا أمام شخصٍ كانت تظنه صبياً في عمرها. فقد تعرضت تود للابتزاز والمضايقة من قبل مهاجمها الافتراضي، ما دفع الطالبة الكندية لإنهاء حياتها. وبقيت القضية عالقة لسنواتٍ عديدة، وبقي والدا أماندا جاهلين لهوية الشخص الذي عذب ابنتهم حتّى شهر نيسان عام 2 عندما قاد تقدم كبير في القضية الشرطة الملكية الكندية إلى هولندا، حيث كان المشبوه على بعد خمسة آلاف ميل. وتمكنت الشرطة الهولندية من

تحديد هوية المجرم الذي كان رجلاً في الخامسة والثلاثين من عمره يُدعى آيدين كوبان، واتهمته "بعددٍ من التهم من ضمنها الابتزاز والتغرير عبر الإنترنت والتحرش وحيازة مواد إباحية للأطفال بهدف التوزيع". اعتمد كوبان في تنفيذ عمليته المفترضة على تأسيس شخصية مزيفة على الإنترنت، والحصول على ثقة الفتيات القاصرات، ومن ثم إغرائهنّ للقيام بحركات جنسية أمام الكاميرا. ويُعتقد أن عشرات الضحايا في كندا وحول العالم تم استهدافهم من قبل هذا الشاذ الهولندي.

حتّى بالنسبة للبالغين، يمكن أن تشكل العلاقات بين الأشخاص والتلاعب بالشاشات مزيجاً خطيراً. وهو ما حدث في قضية إليزابيث ثراشر، التي اتهمت بالتهجّم على ابنة صديقة زوجها السابق. حيث قامت المرأة الغيورة بنسخ صورتين من حساب الفتاة على موقع ماي.سبيس ووضعهما على موقع قائمة كريغ في قسم اللقاءات العفوية. ووضعت أيضاً عنوان منزل الفتاة البريئة ورقم هاتفها وبريدها الإلكتروني ومعلومات مرتبطة بعملها، مدعية أن الفتاة تبحث عن فرص لمؤازرة الجنس. ولم يكن لدى الضحية أي علم بما يجري على الموقع إلى أن بدأت تتلقى اتصالات هاتفية ورسائل نصية وصوراً (من بينها صور عارية) يلتمس أصحابها الجنس. وأدلت الفتاة بشهادتها في المحكمة قائلة إنها كانت تشعر وكأن "أحداً ما كان يعدّها للقتل والاغتصاب".

التلاعب بشاشات الأسهم المالية

ليس الأفراد والشركات هم وحدهم من يقع ضحية التلاعب اعتماداً على ما يظهر عل شاشاتهم، بل ينطبق الأمر على الأسواق المالية أيضاً. ففيما كانت الإشاعات والتخمينات هي التي تحرك الأسواق في الماضي، باتت سرعة الإنترنت الهائلة تجعل العالم يستجيب للمعلومات قبل التحقق من صحتها في أغلب الأحوال. ففي آب عام 2000، أنشأ قرصان اسمه مارك س.جاكوب

في الثالثة والعشرين من عمره، وكان طالباً في جامعة إلسيغوندو الشعبية في ولاية كاليفورنيا، بياناً صحافياً زائفاً وأرسله إلى موقع إنترنت وير، وهو موقع لتوزيع الإعلانات التجارية. وكان جاكوب قد اختار شركة إموليكس، وهي شركة مصنعة لمعدات الاتصالات مدرجة على مؤشر ناسداك، كهدفٍ لهجومه. وقام القرصان بنسخ تنسيق وتصميم بيانات صحافية سابقة لشركة إموليكس، وقلد عنوان البريد الإلكتروني للشركة ليرسل أخباره إلى موقع إنترنت وير. وجاء في البيان الصحافي المخترَع أن لجنة الأوراق المالية والبورصات قد فتحت تحقيقاً يخص شركة إموليكس للمطالبة بتوضيح أرباحها الفصلية من جديد، وأن المدير التنفيذي للشركة بول فولينو قد استقال من منصبه رداً على ذلك. انتشرت هذه القصة المثيرة كالفيروس ليتلقفها العديد من الصحف الإلكترونية مثل ذي.ستريت وسي.إن.بي.سي وبلومبيرغ ودوجونز نيوزويرز.

كانت استجابة السوق متوقعة وسريعة. "فبعد إعادة نشر البيان الصحافي الزائف بست عشرة دقيقة، تم تداول 2.3 مليون سهم من أسهم إموليكس، لينهار سعر السهم بمقدار 61 دولاراً، من 104 دولارات إلى 43 دولاراً، وكانت النتيجة خسارة شركة إموليكس 2.2 مليار دولار من رأسمالها السوقي". وكان ذلك تماماً ما كان جاكوب ينتظره لأنه عندما انخفض سعر الأسهم، حصل هذا الشاب المناور على ربحٍ خفي قدره 250000 دولار. وسارع المدير التنفيذي لشركة إموليكس إلى الظهور على موقع بلومبيرغ وفي بيانٍ صحافي مالي آخر لينكر القصة، لكن الوقت كان قد فات، فقد كان الضرر قد وقع بالفعل. وفي غضون ستة أيام، تمكن مكتب التحقيقات الفدرالي، بالتعاون مع لجنة الأوراق المالية والبورصات، من تحديد هوية جاكوب، الذي اعتُقل واعترف بارتكابه جرم الاحتيال على الضمانات. وبانتهاء القضية، كان المستثمرون الشرعيون في السوق قد خسروا أكثر من

110 ملايين دولار بسبب تلاعب فتى يدرس في الجامعة الشعبية بالثقة التي وضعوها في شاشاتهم.

التلاعب بالشاشات في قطاع الخدمات المالية هو أمر شائع، وتشكّل الخطط المعروفة بخطط "الضخ والتفريغ" العناصر الأساسية في التحايل على الضمانات على الإنترنت. ويقوم بهذه العملية تجار يقومون برفع سعر سهم معين بطريقة مصطنعة، من خلال ضخ تصريحات إيجابية زائفة ومضللة تُوضع على الإنترنت، ومن ثم تفريغ مخزونها من الأسهم العالية السعر عبر بيعها قبل أن تُكتشف كذبتهم. كانت هذه المؤازرة منتشرة في الفضاء السايبري، وقد اعتقل مكتب التحقيقات الفدرالي العشرات من المجرمين لمشاركتهم في مثل هذه العمليات الاحتيالية. وبالرغم من سذاجة طريقة الضخ والتفريغ وبساطة أسلوبها، فإن الأفراد وعصابات الجريمة المنظمة تمكنوا من تحقيق أرباح تُقدر بمئات الملايين من الدولارات عن طريق التلاعب بالمعلومات التي نراها جميعنا على الإنترنت.

يمكن للشاشات المالية أحياناً أن تتلاعب بك بطرقٍ لا يمكنك حتّى أن تدركها، فهي تراقبك بينما أنت تراقبها. هذا ما كان على المتداولين المحترفين في مصرفي غولدمان ساكس وج.ب.مورغان أن يتعلموه حول طرفيات بلومبيرغ للتداول التي واظبوا على استخدامها لسنوات. فمحطات بلومبيرغ هي الدماء التي تضمن حياة وول ستريت، وتنفق الشركات مبلغ 20000 دولار في كل سنة لكل محطة لاستثمار الكميات الكبيرة من البيانات، التي تقدمها في تسيير أعمالهم التجارية اليومية. لكن ما لم يدركه هؤلاء التجار هو أن المراسلين الصحافيين من قسم أخبار لدى بلومبيرغ قد حصلوا على سماحيات إدارية تخولهم مراقبة نشاطات الزبون عندما يستخدم المضاربون صناديق بلومبيرغ التي يوزعونها. بعبارة أخرى، كان المراسلون يراقبون استخدام المحطات لتسهيل إعداد تقارير الأخبار. وكان على التجار

الذين كانوا يظنون أنهم يشاهدون المعلومات ويشاركونها مع محطةٍ بكماء أن يكتشفوا أن المحطة لم تكن كذلك، فقد كانت تراقبهم بالفعل.

ثمة أكثر من 300000 شخص من أكثر الناس تأثيراً في العالم المالي، ومن ضمنهم أصحاب بنوك ومديرو صناديق وقائية ومسؤولون في وزارة الخزينة، يعتمدون على صناديق بلومبيرغ للقيام بأبحاث خاصة للغاية، وترتبط كل عملية من هذا النوع بشخصٍ محدد. وقد خرجت الفضيحة إلى الأضواء عندما قام صحافي من بلومبيرغ بالاتصال ببنك غولدمان ساكس ليستفهم عما إذا كان أحد الشركاء لا يزال يعمل هناك، منوهاً إلى أن الأخير لم يسجل دخوله على الطرفية منذ أيام. وسببت هذه الملاحظة العفوية إطلاق أجراس الإنذار في مصرف غولدمان ساكس الذي خرج بالقصة لينشرها على الملأ.

كُشف لاحقاً أن صحافييّ بلومبيرغ البالغ عددهم 2400 كانوا قادرين على رؤية تاريخ عمليات المستخدمين على محطات الشركة، بالإضافة إلى عمليات البحث المختلفة التي كانوا يستخدمونها، مثل البحث عن الأسهم التجارية والسلع. وقد اشتكى مسؤولو غولدمان من مراسلي بلومبيرغ لتجسسهم على الزبائن الذين يستخدمون محطاتهم، واستغلالهم هذه المعلومات الخاصة للتجسس على نشاطات شركاء غولدمان، وهي معلومات استخدموها لتأليف القصص الإخبارية التي تنشرها شركة بلومبيرغ. وقد سبق أن أشار صحافي سابق في بلومبيرغ إلى أنه "كانت تجري باستمرار مناقشات في غرفة الأخبار عن كيفية استخدام المحطات لكتابة أخبار ضاربة".

يمكن للشاشات المالية أن تتعرض أيضاً للقرصنة والتلاعب عن طريق التداول العالي التردد. ففي كتابه الإبداعي عام 2014، "الشبان الكاذبون"، يروي مايكل لويس كيف قام أفراد من داخل وول ستريت بالتلاعب بنظام

التجارة المالي برمته عن طريق قرصنة الوقت. فعن طريق إنفاق مئات ملايين الدولارات على بنى تحتية متفوقة تقانياً، استطاع متداولو التردد العالي سحب بضعة أجزاء من الثانية من توقيت تداولاتهم، ما منحهم أفضلية على أندادهم أمكنهم استغلالها. ويتابع كتاب "الشبان الكاذبون" براد كاتسوياما، وهو متداول يعمل في مكتب البنك الملكي الكندي في نيويورك، ويرصد ما أجراه من تحقيقات متعددة المستويات مذهلة في تعقيدها استغرقت سنوات في عالم التداول العالي التردد. وكان ما اكتشفه صاعقاً: ليست سوق الأوراق المالية كما تظهر على الشاشات سوى وهم.

كما اتضح، فإنه في كل مرةٍ كان يحاول فيها كاتسوياما القيام بعملية تجارية، كان ثمن السهم يتحرك قبل أن يكمل طلبه. فكيف كان ذلك يحدث؟ لقد اكتشف متداولو السرعات العالية طريقة لاستغلال السرعات المختلفة التي تنتقل بها المعلومات التجارية عبر أسلاك الألياف البصرية إلى سوق الأوراق المالية. وبالرغم من أن الإشارات تنتقل بسرعة تعادل ثلثي سرعة الضوء، فإنه يتم إضافة الفوارق الزمنية الصغيرة للمسافات الأطول، بحيث يمكن الاستفادة منها. وبدفع كميات كبيرة من الأموال من أجل الحصول على أسرع الأسلاك وأقوى الحواسب وامتياز مشاركة مخدمات البيانات مع البورصة في المكان نفسه، كان التجار السريعون قادرين على معرفة نية كاتسوياما بشراء سهم بسعر مميز، ليقوموا بشرائه قبله ومن دون علمه وبالسعر الظاهر أمامه على شاشته. لم يكن كاتسوياما الضحية الوحيدة، فقد تأثرنا جميعاً بالمشكلة نفسها؛ لكنه كان أول من وثقها. كان متداولو التردد العالي يستبقون السوق ليخدعونا جميعاً ولتطال خدعهم مشترياتك التأمينية وخططك الضريبة، بل خطط توزيع المعاشات في المدينة.

قام متداولو التردد العالي بقرصنة الوقت والشاشة، وهي طريقة تصنّف

تحت هجومات الوسيط. فهم يقحمون أنفسهم بين بيانات البورصة التي يفترض أن تصل بالزمن الحقيقي لتعرض على شاشة كاتسوياما وبين الواقع الأسرع، الذي يسيطرون عليه ويتحكمون به. فقد كانت حواسبهم سريعة جداً، بما مكنهم من تحديد طلبات الناس والمضي قبلهم لشراء الأسهم المتوفرة ومن ثم بيعها للشخص نفسه الذي حاول شراءها في الأصل، لكن بسعرٍ أعلى. وتجميع بضعة بنسات من هنا وهناك من خلال ملايين العمليات التجارية في اليوم الواحد سمح لمتداولي التردد العالي بالحصول على مليارات الدولارات كأرباحٍ تراكمية، من خلال أفضلية تجارية تعتمد على خمسة أجزاء من الثانية. وللإحاطة بمقدار السرعة، فإن ومضة العين تستغرق تقريباً ثلاثمئة إلى أربعمئة جزء من الثانية. الأمر أشبه بمشهد في فيلم المصفوفة (The Matrix)، حين يقوم الأشرار بالبدء بإطلاق النار على بطل الفيلم نيو (الممثل كيانو ريفز)، بينما يتمكن الأخير من رؤية الرصاصات تدنو منه ليتحرك بسرعة الضوء تفادياً لها. لكن الأمر مختلف هنا، فهو يتعلق بقرصنة الأنظمة المالية، وما من أحد منّا، نحن الأفراد البسطاء، يمتلك القوى التي يتمتع بها نيو.

خلال الأيام التي تلت نشر كتاب "الشبان الكاذبون"، أُجريت سلسلة من التحقيقات من قبل لجنة الأوراق المالية والبورصات ومكتب التحقيقات الفدرالي والنائب العام لولاية نيويورك. لكن اهتمامهم المفاجئ أثار سؤالاً هاماً: كيف يمكن لهذا النظام أن يتطور أصلاً تحت مرأى لجنة الأوراق المالية والبورصات وفي أعقاب الأزمة المالية العالمية عام 2008؟ لقد أشار مايكل لويس عن حق إلى أن "السوق مزورة"، لكن قبل أن يصبح ذلك ممكناً، كان لا بد للشركات المشتركة في هذا النوع من التداول أن تتدبر أمر شاشتك لكي تختلق قصتها الخيالية عن السوق الموثوقة والشفافة. ومن المزعج أن نعرف أننا نعيش في عالم تكون فيه شاشات المستشفيات

والسجون وأقسام الشرطة والمصارف وشركات الوساطة ومواقع الأخبار هدفاً سهلاً للقرصنة، لكن الشاشات، كما سنرى، تزداد انتشاراً والتهديدات تتعاظم والهجمات قد تكلفنا أكثر بكثير من المال.

الفصل التاسع

مزيدٌ من الشاشات يعني مزيداً من المشاكل

> في عالمٍ يزداد ابتعاداً عن الحقيقة كل يوم، يزداد عدد أولئك الذين يتقبلون الافتراضي أكثر من الحقيقي، وكل الأشياء الافتراضية مطاطة.
>
> دين كونتز، الرجل الطيب

كانت روبين سيج امرأة شابة وجذابة في الخامسة والعشرين من عمرها، تعمل كمحللةٍ للتهديدات الإلكترونية في قيادة العمليات الحربية الإلكترونية للبحرية الأميركية. وكان لديها شهادات من معهد ماساتشوستس للتكنولوجيا وتدربت في وكالة الأمن القومي. مثل كثير ممن في عمرها، كانت روبين مستخدمة ماهرة لشبكات التواصل الاجتماعي، وكان لديها حسابات على الفايسبوك ولينكدإن وتويتر. وبعد أن بدأت حياتها العملية في البحرية بوقتٍ قصير، أخذت ترسل طلبات الصداقة إلى محترفين إلكترونيين آخرين يعملون في الحكومة. وفي أقل من شهر، ضاعفت حجم معارفها في الشبكة لتصل إلى أكثر من ثلاثمئة جهة اتصال في عالم الحماية الإلكترونية، من بينها موظفون عسكريون ومسؤولون في الدفاع ومجموعة من الموظفين في وكالاتٍ استخبارية متنوعة. وكان من بين أصدقائها على الإنترنت رئيس قسم المستشارين ورئيس قسم المعلومات في وكالة الأمن القومي وموظفون استخباريون رفيعو المستوى في فيلق البحرية ورئيس هيئة أعضاء الكونغرس الأميركي، ومديرون في كل من لوكهيد مارتن ونورثروب غرومان وبوز ألين هاميلتون.

مع أن الذين تلقوا طلبات الصداقة لم يتذكروا المرأة الشابة في البداية، فإن روبين أكدت لهم أنها قابلتهم جميعاً في العام المنصرم في مؤتمر DEF، وهو اجتماع واسع وضخم للقراصنة تتردد عليه مجموعات القراصنة وأعضاء الحكومة على حد سواء. وقام أولئك الذين كانت لديهم شكوك

دائمة فقط بالاطلاع على شبكة روبين ليروا كم لديهم من الأصدقاء المشتركين، ما خفف مخاوفهم من قبول طلبات الصداقة التي أرسلتها إليهم. كما أقامت روبين صداقات على الفايسبوك ولينكدإن مع أولئك الذين يعملون معها في البناء نفسه في قيادة العمليات الحربية الإلكترونية للبحرية. وعندما بدأ وجودها على شبكات التواصل الاجتماعي يزداد، أصبحت شركات مثل لوكهيد مارتن وغيرها مهتمة في تشغيل الشابة للعمل لديها، وبدأت عروض العمل تنهال عليها. كانت ثمة مشكلة بسيطة فقط، وهي أن روبين سيج لم تكن موجودة.

كانت سيج مجرد اختراع من قبل توماس ريان، وهو مستشار أمني أراد من هذه الخطوة أن يختبر التهديدات التي تفرضها الوسائط الاجتماعية على المحترفين العاملين في المنظمات الأمنية الوطنية. وكان هدفه بسيطاً، وهو رؤية ما باستطاعته جمعه سراً من معلومات استخبارية عن طريق شبكات الوسائط الاجتماعية بواسطة شخصية خيالية. وفي أقل من شهر، بدأ أصدقاؤه الجدد مشاركة بيانات على نحو واسع مع شخصيته البديلة الجذابة، روبين سيج. وباستخدام فنانته الافتراضية، استطاع ريان خداع أحد أفراد قوات الصاعقة الأميركية، الذي ضمن قائمة أصدقائه، بحيث جعله يرسل لسيج صوراً تحتوي على بيانات جغرافية مضمّنة فيها عن قاعدته السرية في أفغانستان. وقام الجندي أيضاً بكشف تفاصيل عن تحركاته وتحركات قوات أخرى في العراق لـ "صديقته" الجديدة.

كان حضور روبين سيج على الشاشات مقنعاً لدرجة أنها تلقت وثائق سرية لتراجعها، بالإضافة إلى عروضٍ لإلقاء كلمات في مؤتمرات مرموقة عن الأمن والحرب السايبرية. فما مدى الصعوبة التي واجهها ريان في تنفيذ حيلته ضد مجموعة نخبوية من المحترفين العسكريين والاستخباريين الناضجين الذين يعملون في الأوساط الأمنية الوطنية الأميركية؟ كان الأمر

سهلاً جداً. فكل ما قام به ريان هو التقاط صورة من الإنترنت لاستخدامها في إنشاء حسابات لسيج على مواقع التواصل الاجتماعي. وكانت الصورة في الحقيقة تعود إلى نجمة إباحية غير مشهورة. وحتى الاسم، روبين سيج، كان في الواقع اسماً لتدريب عسكري ضخم يجري سنوياً من قبل الجيش في كارولينا الشمالية. أما عنوان روبين فكان عنوان شركة التعهدات العسكرية الأمنية الذائعة الصيت بلاك ووتر. وأثبتت تجربة روبين سيج كم يستهان بالثقة التي يضعها الناس في الشاشات. وإن كان رجال الجيش والاستخبارات المدرّبون قد وقعوا في هذا الفخ، فأية إمكانيات تتوفر لعامة الناس لكي يحموا أنفسهم من مثل هذه التهديدات؟ ولكن عندما يكون كل شيء متصلاً، تصبح الحواسب بعيدة كل البعد عن أن تكون مجرد شاشات.

فلترة المكالمات الهاتفية

نظراً إلى الانفجار الذي يشهده انتشار الأجهزة النقالة، ليس من المفاجئ أن يحول المجرمون اهتمامهم عن الشاشات الكبيرة ليضعوه في تلك الأصغر حجماً، وخاصة أن برامج الهواتف النقالة أقل حماية من نظيرتها على الحواسب المكتبية. وبالرغم من أننا اعتدنا مشاهدة شاشات تحديد هوية المتصل على هواتفنا وفي مكاتبنا ومنازلنا، فإنها مثل بقية الشاشات من السهل اختراقها. وهنالك عدد كبير من البرامج والمواقع الإلكترونية التي أُنْشئت لتبديل هوية المتصل في المكالمات الهاتفية الصادرة.

تجعل مواقع إلكترونية وتطبيقات مثل SpoofCard.com وSpoofTel.com عرض رقم مختلف في أي اتصال هاتفي صادر في غاية السهولة. فكل ما عليك القيام به هو إدخال الرقم الذي تريده أن يظهر على أنه الرقم الذي تتصل منه وكذلك اسم جهة الاتصال، ليتم عرضهما كما هما على شاشة تحديد هوية المتصل لدى الشخص الهدف. أتريد أن تتظاهر بأنك الرئيس؟ لا مشكلة في ذلك، فقط قم بإدخال الرقم

"202-456-1414" واسم "البيت الأبيض" في التطبيق وسيفي ذلك بالغرض. تقدّم شركات تقليد رقم المتصل بالهاتف باقة متنوعة من العروض غايتها خداع الأحاسيس الأخرى غير البصر. إذ تقدم هذه الشركات أيضاً للمستخدمين القدرة على تغيير الصوت من الذكوري إلى الأنثوي، بل إدخال أصوات كخلفية لأية محادثة لإقناع الطرف الآخر بأنك تتكلم من مكتبٍ مزدحم أو ملهى ليلي أو أثناء وجودك في زحمة سير أو في المطار. وتبيع هذه الشركات مثل هذه المنتجات كوسيلةٍ "لحماية هويتك" أو "لتمرير مزحة على أصدقائك". ويمكن بالطبع التلاعب بالرسائل النصية أيضاً باستخدام التقنيات نفسها. ما من شك في أن المراهقين سيجدون متعة بالتظاهر بأنهم شخص ما مثل ليدي غاغا أو مدير في مكتب التحقيقات الفدرالي، إلا أنه ثمة استخدامات مريبة واضحة يتوق المجرمون إلى استغلالها.

في الفضيحة المدوية للاختراق الهاتفي لشركة الأخبار نيوز كورب، سمحت شاشة تقليد هوية المتصل للصحافيين بالدخول إلى نظام البريد الصوتي لميلي دولر وآخرين غيرها، وهو هجوم من السهل أن يحدث بسهولة معك أيضاً. ونجحت الحيلة حيث الكثير من مشغلات الهواتف النقالة لا تفرض استخدام كلمة سر للدخول إلى صندوق البريد الصوتي. ويعتمد النظام فقط على معرّف هوية المتصل لتشغيل رسائلك. بما أن جميع شركات الهاتف النقال في العالم لديها 800 رقم أساسي يمكنك الاتصال بها لمراجعة رسائلك عندما تستخدم الهاتف الثابت، فإن الأشرار يقومون فقط بتقليد رقمك الصادر عند القيام بالاتصال بنظام البريد الصوتي لشركة الهاتف النقال، وبهذه البساطة يمكنه التمتع بحرية الدخول إلى رسائلك. ولم يكن عامة الناس في المملكة المتحدة هم من استُهدِفوا بهذه التقنية، بل قام بعض المشاهير أيضاً باستخدامها ليخترقوا البريد الصوتي لخصومهم باحثين عن

الشائعات، تماماً كما فعلت باريس هيلتون عندما استخدمت تطبيق سبوفكارد للاستماع إلى رسائل ليندسي لوهان.

وبالعودة إلى العالم الحقيقي لعامة الناس، يعني تقليد هوية المتصل أن المجرمين بإمكانهم الإصغاء إلى رسائلك في المكتب ومعرفة معلوماتٍ قيّمة تتعلق بصفقاتٍ تجارية معلّقة وباندماج الشركات ومكاسبها، بل حتّى بياناتٍ شخصية طبية. ومن منظورٍ اجتماعي هندسي، يخلق التقليد الهاتفي أداة قوية للتفكير الإجرامي. إن مكالمة هاتفية مُقلّدَة لقسم تكنولوجيا المعلومات في شركة تطلب إعادة كلمة سر النظام أو أحدث مفتاح للشبكة اللاسلكية، تكون أكثر نجاحاً إذا تبين أن المكالمة صادرة من البنية التحتية الهاتفية لهذه الشركة بالذات، وهي حيلةٌ لطالما كانت ناجعة.

وعلى مستوى الأفراد، يمثل خداع شاشة هاتفك النقال بهوية متصل مُقلّدَة أداة مثالية للاحتيال المصرفي. إذ تقدم المؤسسات المالية مثل بنك أميركا وتشيس خدماتٍ مصرفية هاتفية، ويقوم المجرمون باستمرار بتقليد رقم الهاتف الخاص بالحساب الذي يرغبون بالدخول إليه. فعندما يرى نظام البنك الهاتفي مكالمة قادمة من رقم هاتفك، فإن كل ما يحتاج إليه الأشرار هو بضع معلومات شخصية (كالأرقام الأربعة الأخيرة من رقم الضمان الاجتماعي الخاص بك أو اسم عائلة والدتك)، وهي معلومات يمكن الوصول إليها بسهولة في الأوساط السرية الرقمية أو عبر حسابك على الفايسبوك، وهي موجودة حقاً. والأسوأ من ذلك هو أنه بإمكان المجرمين تقليد رقم هاتف مصرفك والاتصال بك للحصول على معلومات كالأجوبة على أسئلة الحماية مثلاً، ليتجهوا بعدها للاتصال بالبنك مستخدمين رقم هاتفك النقال المُقلّد وبيانات الضمان التي قدمتها لهم ببراءة ليدخلوا إلى حسابك.

تمكنت عصابات الجريمة المنظمة من أن تقلد حتى المكالمات الصادرة

للحكومة الفدرالية وجنت الملايين من وراء ذلك. ففيما وصفته مصلحة العوائد الداخلية بأنه أضخم عملية احتيال ضريبي حتى الآن، قام المحتالون بتقليد رقم هاتف الوكالة ليتصلوا بك. أما أنت فترى مكالمة واردة من مصلحة الضرائب وتتساءل، آه، يا للحماقة... ما القصة؟ وعلى الطرف الآخر من الخط تجد عميل مصلحة الضرائب يبلغك بأنك مُقصر في سداد ضرائبك وأن عليك أن تدفع حالاً لمصلحة الضرائب، لكي لا تتعرض لمزيد من العقوبات. ويتم إخبار الضحايا بأنه "استناداً إلى حدة الجريمة وإلى حالة التقصير السابقة لديك، لن نقبل أن تدفع سوى عن طريق برقية مصرفية أو بطاقة ائتمانية". ولإضافة صدقية إلى الحيلة، يقوم عميل مصلحة الضرائب المزعوم بتأكيد الأرقام الأربعة الأخيرة من رقم الضمان الاجتماعي لدافع الضرائب (والذي تسرب من خلال إحدى اختراقات البيانات الكبيرة التي تطرقنا إليها سابقاً). أما أولئك الذين يشككون بموظف مصلحة الضرائب المفترض عبر أسئلتهم فيقابلون بوابلٍ من التهديدات مثل الاعتقال وإلغاء إيرادات عملهم أو رخص قيادتهم، بل وحتّى الترحيل إذا كان الاسم يبدو أجنبياً.

دعم المحتالون صدقية ادعاءاتهم عن طريق قرصنة شاشات أخرى وبإضافة بعض الممثلين إلى الخدعة. فبعد تلقيهم للمكالمات الهاتفية، يتلقى الضحايا بريداً إلكترونياً يبدو رسمياً ويحمل عنوان مصلحة الضرائب، يؤكد المكالمة الهاتفية ويطلب دفعة من النقود. ويتلقى الضحايا أيضاً مكالماتٍ إضافية من أقسام الشرطة المحلية مع هوية المتصل المُقلّدَة (مثل قسم شرطة أميريست في ولاية ماساتشوستس) أو من موظف مزعوم في قسم المركبات في الولاية (مثل قسم مركبات ولاية جورجيا). وتؤكد جميع هذه الإضافات الرسمية الحيلة من خلال عبارات مثل "هنا المحقق سميث من قسم شرطة أميريست. لقد تلقينا إشعاراً من مصلحة الضرائب يقول

إنك مقصر في دفع الضرائب وإن المبالغ مستحقة السداد جنائياً. أرجو ألا أجد نفسي مجبراً على القدوم لاعتقالك أمام عائلتك. وإذا كان باستطاعتك الدفع هذا الأسبوع، فلقد أبلغتني مصلحة الضرائب أنه لا ضرورة لاعتقالك". ووفقاً للمفتش العام لقسم الخزينة، فإن أكثر من عشرين ألف شخص قد وقعوا ضحية هذه الخدعة.

قد لا يكلفك الإيمان بالشاشات نقودك فحسب، بل من الممكن أيضاً أن يكلفك حياتك. ففي ظاهرةٍ تُعرف باسم الاقتحام العنيف، كان بمقدور القراصنة الضجرين أن يتصلوا برقم الشرطة 911 الخاص بالطوارئ، باستخدام هويات هاتفية مُقلّدَة لكي يبلغوا عن جرائم غير موجودة، والنتيجة هي استجابة فرق المهام الخاصة مدججة بالسلاح. وحتى إذا كان القرصان في ولاية ماين، فإن استخدامه لرقم هاتفك في ولاية ميامي سيدفع الشرطة إلى التوجه إلى هناك. وتبدأ اللعبة القاتلة عندما يقلّد المجرمون رقم هاتفك ويتصلون بالرقم 911 وتصرخ امرأة على الهاتف "أطلق زوجي النار على أمي وطفلي، وهو يتخذني الآن رهينة، أرجوكم أسرعوا... إنه يحمل بندقية صيد وأخرى من نوع AK-47... أسرعوا... إنه مجنون!". ويمكن تشغيل أصوات عيارات نارية في خلفية الاتصال لمزيد من الإقناع، وعندها يكون الفخ القاتل قد نُصب.

في هذه الأثناء، تكون أنت جالساً في منزلك على الأريكة تأكل المثلجات مع زوجتك وأولادك، وتستمتعون بمشاهدة آخر حلقة من برنامج بيغ بانغ ثيوري، بينما يعتقد رجال الشرطة أن المرأة في الداخل تفصلها عن الموت بضع لحظات، فيجمعون كافة المركبات المتوفرة ووحدة المهام الخاصة ليأتوا وينقذوها. عندما يلتقي الطرفان يكون هنالك سوء فهم هائل يجعل اللقاء قابلاً للانفجار. يطوّق رجال الشرطة المنزل ويبدأون بالمناداة عليك لتخرج ويداك مرفوعتان نحو الأعلى. أطفالك يصرخون وزوجتك مضطربة.

لكنك لا تستجيب لأوامر الشرطة ما يزيد من شكوكهم بأن شيئاً مشبوهاً يدور داخل المنزل. لكنك لا ترغب بالخروج من المنزل لتواجه مجموعة من المجانين (حتى لو كانوا من رجال الشرطة) يصوبون بنادقهم باتجاهك. أما بالنسبة للشرطة فإن رفضك التعاون معهم يزيد من حالة التوتر. وستكون خطوتهم التالية هي إطلاق بعض القنابل الصوتية عبر نافذة منزلك وانتظار ما سيحدث. أو ربما كنت بدلاً من ذلك تغط في نومٍ عميق عندما قام القرصان المراهق من على بعد عدة ولايات عنك بتطبيق حيلته. يصل رجال الشرطة، وتوقظك الضجة خارج المنزل. تظن أنه ثمة لصوص، فتمسك ببندقيتك وتخرج للتحقق من الأمر. الآن، وقد خرجت من المنزل وبيدك بندقية، تجد أمامك ستة عناصر من فريق المهام الخاصة المحلي يوجهون ضوء الليزر الأحمر إلى جبينك. لا يمكن لمثل هذا السيناريو أن ينتهي بسلام.

سجل مكتب التحقيقات الفدرالي ما لا يقل عن أربعمئة حادثة اقتحام عنيف في عام 2013 لوحده أوقعت ضحايا في جميع أنحاء البلاد، من أوهايو وحتى كاليفورنيا. ويقوم القراصنة بذلك في أغلب الأحيان من باب "التسلية" لأنهم يستطيعون ذلك. في الأيام التي سبقت ظهور الإنترنت، كانت خدعة المراهقين الكبرى هي طلب طبق من البيتزا وإرساله إلى فتى لا يحبونه في المدرسة. أما الآن فأصبح الأولاد يأمرون وحدات المهام الخاصة بسلاحهم لينفذوا مزاحهم وخدعهم. ففي عام 2009 على سبيل المثال أُدين مجموعة من المراهقين بارتكاب أكثر من ثلاثمئة هجوم اقتحام. ففي بعض الحالات كان المراهقون يقابلون ضحاياهم على مواقع التواصل الاجتماعي أو مواقع المواعدة وينتقمون منهم إذا رفضوا، على سبيل المثال، المشاركة في محادثاتٍ جنسية. ليس الاقتحام العنيف في الحقيقة سوى الوجه الآخر للإعلانات الجنسية الكاذبة على موقع قائمة كريغ التي يضعها العشاق السابقون الغيورون للانتقام من شركائهم السابقين معرضين إياهم لمخاطر

أكبر مما يتصوروا.

يتعرض المشاهير والشخصيات العامة المعروفة للاستهداف بمثل هذه الممارسات على نحوٍ متزايد. ففي عام 2013، تمت مقاضاة فتى من لوس أنجلوس يبلغ من العمر اثني عشر عاماً بتهمة تنفيذ خدعة الاقتحام العنيف على منزل أشتون كوتشير في هوليوود، وعلى أرض عائدة لجاستن بيبر في كالاباساس في ولاية كاليفورنيا. ونفذ الصبي الخدعة أيضاً على مصرف محلي مدعياً حدوث عملية سطو. وهنالك العديد من المشاهير الذين وقعوا ضحايا هذه الخدع، ومن بينهم روسيل براند وتوم كروز وريهانا وتشارلي شين وميلي سيروس. ومعجزة أنه لم يُقتل أحد من المدنيين الأبرياء نتيجة لحوادث الاقتحام هذه، بالرغم من أن العديد من ضباط الشرطة قد جُرحوا معرضين حياتهم للخطر عند استجابتهم السريعة للمكالمات المُقلّدَة الرهيبة التي تطلب النجدة على الرقم 911.

ثمة طريقة أخرى يتبعها المجرمون للتحايل على شاشة هاتفك، وهي الهجوم على نطاق الاتصالات القاعدي فيه، والتي تمثل الأقسام الداخلية المسؤولة عن تشغيله الفعلي وعن معالجة كافة الاتصالات بين ما تراه على شاشتك وبين مجموعة من الهوائيات الراديوية التي تتحكم بكل شيء، بدءاً بالرسائل النصية التي تتلقاها ووصولاً إلى المكالمات الصوتية وإشارات الواي فاي، بالإضافة إلى بروتوكولات الاتصالات المتقدمة مثل النظام العالمي للاتصالات الخلوية ونظام الجيل الثالث للاتصالات الخلوية يو.إم.تي.إس ونظامي إتش.إس.دي.بي.إيي وإل.تي.إي. ولأن نطاق الاتصالات القاعدي هو نطاق احتكاري وليس عامَّ الملكية، فإن معظم الشركات المصنعة لأجهزة الهاتف تطبق أنظمة التشغيل المبيّتة هذه بطريقة غير آمنة. فهؤلاء يؤمنون بالحماية عن طريق الإغفال وكأن لسان حاله يقول إن هذا البرنامج بعيد عن الأنظار إلى حد لا يمكن معه لأحد ملاحظته، ولذلك فليس من

الضرورة الاهتمام كثيراً بالحماية. هذا هو منطقهم، لكنهم مخطئون بالطبع.

بدأ عددٌ من القراصنة والحكومات والباحثين الأمنيين بالنجاح في تفكيك رقاقات وشفرات النطاق القاعدي، ليكشفوا عن حزمةٍ واسعة من نقاط الضعف التي يمكن استخدامها للدخول إلى بيانات الهاتف وتعديلها عن بُعد. ففي بداية عام 2014، وُجد مثل هذا الخلل الأمني في نظام الاتصال القاعدي لهواتف سامسونج غالاكسي، وكان يسمح للقراصنة بالدخول إلى بيانات المستخدم المخزنة على الأجهزة. ولأن أجهزة الهواتف الذكية هي ليست إلا حواسب مصغرة، فإن شاشاتها مثل شاشات أخوتها الأكبر يمكن التلاعب بها بحيث تعرض واقعاً مُعدّلاً بغية الاحتيال. وتفيد التقارير بأن مكتب التحقيقات الفدرالي قد استخدم هذه التقنية لتحويل الهواتف إلى أجهزةٍ للتجسس وذلك بتعديل الواجهة الاعتيادية للهاتف وجعله يجري اتصالاً سرياً بمكتب التحقيقات الفدرالي، ما يسمح بالمراقبة عن بعد. بعبارة أخرى، حتّى عندما لم يكن الجهاز يُظْهِر سوى شاشة التطبيقات الخاصة بك، فإنه كان في الواقع على اتصال هاتفي بضباط مكتب التحقيقات الفدرالي الذين يستمعون إليك.

يمكن للمجرمين بدورهم أن يتلاعبوا بهذه الشاشات بالطريقة نفسها مستخدمين تقنيات لا يمكنك توقعها أبداً. فعندما تُجري اتصالاً برقم ما على هاتفك على سبيل المثال، فإنك تضغط على سلسلةٍ من الأرقام على شاشتك لكي تتصل بالشخص المطلوب. ولكن كيف لك أن تعرف أن الرقم الذي طلبته هو الرقم نفسه الذي كنت متصلاً به؟ سيكون الأمر بسيطاً عندما تتصل بوالدتك وتلقت هي مكالمتك. ولكن ماذا إذا كنت تتصل بسيتي بانك أو بنك أميركا أو ويلز فارغو؟ لن تصل إلى صاحب البنك في أحد الفروع المحلية بالطريقة التي كنت تتبعها منذ عشرين عاماً. فبدلاً من

ذلك، سيتم توصيلك بشخصٍ لم يسبق لك أن حدثته من قبل في مركز الاتصالات، وعادة ما يكون في بلدٍ أجنبي مكون من فريق عملٍ ذي لهجاتٍ أجنبية.

باستخدام البرمجيات الخبيثة للهواتف النقالة، يمكن للقراصنة تنصيب فيروس "روتكيت" على جهازك، ما يمنحهم سيطرة كاملة على كافة خصائص الهاتف بما فيها شاشة اللمس ولوحة الأرقام. هذه البرمجيات الخبيثة هي برامج تخفي العمليات والوظائف الطبيعية للحاسب عن نظر المستخدم وتمنح القراصنة دخولاً إدارياً إلى أي جهاز. وتعرف عصابات الجريمة المنظمة الأرقام الثمانمئة العائدة لمؤسسات مالية حول العالم. فإذا أُصيب هاتفك ببرمجية خبيثة، وبمجرد طلبك لرقم خدمة الزبائن في المصرف، يكتشف الفيروس أن إحدى المؤسسات المالية المستهدفة يتم الاتصال بها الآن ويمكنه عندها اعتراض المكالمة وتحويلها. إنه هجوم تقليدي آخر من نوع "الرجل الوسيط" يسمح للمجرمين بصياغة وتجسيد الواقع الذي تراه على شاشتك وإخضاعه لنتيجتهم المرجوّة.

وبالنتيجة، عندما تطلب رقم المصرف، يتم تحويل اتصالك خفيةً إلى مركز اتصالات، تديره وتشرف عليه عصابة إجرامية عالمية منظمة. ومع الاستخدام الواسع لمراكز الاتصالات الأجنبية من قبل المؤسسات المالية، لماذا تكترث للهجة من هو على الطرف الآخر من الخط عندما تتصل بالبنك الذي تتعامل معه؟ سيكون من السهل نسبياً تنفيذ عملية التقليد. وحالما يتم الاتصال، سوف يتم سؤالك عن رقم حسابك واسم عائلة والدتك وكلمة السر وغيرها من المعلومات الأمنية الأخرى "وذلك فقط للتحقق من هويتك". وبعد ذلك سيتم إخبارك، "عذراً سيدي، لقد تعرضت حواسبنا لعطل فني، وأخبرنا قسم الصيانة أنه سيتم إصلاح العطل وستكون الحواسب جاهزة غداً صباحاً، هل يمكنك الاتصال ثانية؟". لن يجد أي

شخص تعامل في السابق مع موظفي مركز الاتصالات ما يدعو للشك في تلك المحادثة. لكن الاختلاف الوحيد هو أنه مع نهاية المكالمة الهاتفية سيكون المجرمون قد دخلوا إلى التفاصيل المصرفية والشخصية واستخدموها بسرعة ليفرّغوا حسابك من كافة محتوياته. كل ذلك ممكن لأن شاشات هواتفنا لا ترينا الواقع بل قيمة تقريبية تكنولوجية له. لذا فإنه من الممكن قرصنة لا معرّف هوية المتصل ونظام التشغيل على الهاتف وحسب، بل ميزات أخرى منها وحدات تحديد الموقع الجغرافي جي.بي.إس. نعم هذا صحيح حتّى موقعك يمكن تقليده.

ضائع في الفضاء: قرصنة الموقع الجغرافي

في فيلم جيمس بوند عام 1997، الغد لن يموت أبداً، نجد السيد بوند يحقق في هجوم تشويشٍ على نظام الملاحة والموقع الجغرافي لبارجة حربية بريطانية. وفي مجريات القصة، يتعرض نظام الملاحة الخاص بالسفينة ديفونشير للتلاعب من قبل شخص عبقري شرير يستخدم "صندوق تشفير" ليغير مسار السفينة. وتدخل ديفونشير بذلك المياه الإقليمية الصينية ويبدو أنها تغرق بعد استهدافها من قبل أسطول البحرية الصيني. على أية حال، بالنسبة للبريطانيين كانت السفينة في المياه الدولية، ولذلك فإن ما قام به الصينيون يعتبر بمثابة إعلان حرب. أما أفعال ذلك الشرير فكانت لها غاياتها وهي دفع بريطانيا والصين إلى الحرب. مرة أخرى تتنبأ هوليوود بالشر المستقبلي على طريقتها.

نظام الموقع الجغرافي العالمي هو نظام يعتمد على مجموعة من أربعة وعشرين قمراً اصطناعياً ملاحياً فضائياً تعمل في مدار منخفض، توفّر معلومات الوقت والموقع في أي مكانٍ على الكوكب. إنه "مرفق خفية" نعتمد عليه في التجول في أنحاء المدينة وفي تسليم الطرود البريدية وفي العثور على أقرب مقهى وفي تنسيق الملاحة الجوية وفي إدارة السلامة

العامة، بل في توجيه الصواريخ أيضاً. لقد ولى زمن الخرائط الورقية وبتنا نعتمد على شاشات الملاحة التي نراها كل يوم أمامنا مفترضين أن الحاسب هو أفضل من يعلم. أما في الواقع، فتتوالى الأمثلة حول العالم عن سائقين اتبعوا بشكل أعمى شاشات الملاحة بدلاً من الاعتماد على عيونهم، وكانت النتيجة دخولهم في الاتجاه الخطأ في طرق ذات اتجاه الواحد أو حتى خروجهم عن الجسور. ففي إسبانيا، عندما طلب جهاز الموقع الجغرافي إلى السائق بأن ينعطف نحو اليمين، وافق الأخير لينتهي في بحيرة لاسيرينا، وهي أضخم مياه في غرب إسبانيا. وبينما نجا المسافر المرافق، غرق السائق، وكل ذلك لأنه اتبع توجيهات الشاشة التي أمامه.

حذّر تقرير لوزارة الداخلية الأميركية من أن البنية التحتية الحساسة لأميركا "في خطرٍ متزايد نتيجة الاعتماد الكامل على نظام الموقع الجغرافي في تحديد الأماكن والملاحة". وكان الإصدار الصحافي لتقرير مشابه أعدته الأكاديمية الملكية للهندسة في المملكة المتحدة أشد لهجة في تقديره للموقف حيث بيّن أنه: "قد كان المجتمع يبالغ بالفعل وعلى نحو خطير في اعتماده على أنظمة الأقمار الصناعية للملاحة مثل نظام الموقع الجغرافي... ويمكن أن يؤدي خطأ في الإشارة أو التشويش إلى التأثير على أنظمة السلامة والأقسام الحساسة للاقتصاد". وسرعان ما يتضح أن البنية التحتية لسلسلة الأنظمة اللاسلكية والأقمار الصناعية لا تختلف عن البنية التحتية الإلكترونية من حيث ضعف الحماية والانفتاح الكبير وإمكانية التعرض للقرصنة.

نظام الموقع الجغرافي هو إنجاز تكنولوجي رائع، لكن الإشارات الحقيقية لنظام جي.بي.إس التي نتلقاها من الأقمار الصناعية، وإن كانت تعمل جيداً، ضعيفة، وهي أشبه برؤية الضوء العلوي لمركبة من مسافة اثني عشر ألف ميل. ولا يمكن دفع هذه الإشارات لمسافةٍ أبعد بسبب الطاقة

المحدودة لأي من الأقمار الصناعية المشاركة. والأسوأ من ذلك بعد هو أنه يمكن وبسهولة التغطية عليها عبر بث الضجيج على التردد نفسه، بما يسمح بعرقلة عمل الأجهزة الموجودة على الأرض ومنعها من استقبال المعلومات الملاحية.

كانت القوات العسكرية الخبيرة في فن "الحرب الإلكترونية" في السابق هي الوحيدة التي تتوفر لديها التقانة والخبرة الضروريتان للتشويش على إشارات جي.بي.إس، الأمر الذي كانت له آثاره الاستراتيجية الواضحة. فإذا كان بمقدورك عرقلة أنظمة ملاحة عدوك، فيمكنك عندها الاطلاع على تحركات جيوشه وسفنه ودباباته وأسطوله البحري. ويمكنك أيضاً أن تخرب البنية التحتية المدنية الوطنية لعدوك تخريباً كبيراً. وهو ما سبق أن عشناه في الولايات المتحدة الأميركية عام 2007 في مدينة سان دييغو بكاليفورنيا، عندما عانت المدينة كلها "عطلاً إلكترونياً مفاجئاً". فبحلول الظهيرة، وجد المشرفون على الحركة الجوية أن أنظمتهم بدأت تتخبط في عملها. وفي المستشفيات المحلية، توقفت أجهزة البيجر التي يستخدمها الأطباء عن العمل. وفي ميناء سان دييغو بدأ يضطرب عمل نظام الملاحة. وتوقفت الهواتف الخلوية في المدينة عن العمل لمدة ساعتين كاملتين، وتوقفت الصرافات الآلية عن تقديم النقود. كانت هذه الحالة التي أصابت أجمل المدن الأميركية أشبه بأحد أفلام بروس ويليس. ولكن ما الذي سبب هذا الانقطاع الهائل للخدمة؟ بقي هذا الحدث لغزاً لمدة ثلاثة أيام إلى أن تقدمت البحرية أخيراً باعتراف بقيامها بمناورة عسكرية تدريبية لاختبار تقنية جديدة للتشويش الراديوي.

لكن التشويش العسكري على إشارات جي.بي.إس لا يتم دائماً بالمصادفة. فقد درجت كوريا الشمالية على مهاجمة جارتها الجنوبية وحجب إشارات جي.بي.إس الخاصة بها. وتستخدم بيونغ يانغ ثلاثة أجهزة تشويش كل منها

بحجم مقطورة جرار، يمكنها إعادة تمركزها لكي تشوش على أكبر قدر ممكن من المعلومات الملاحية القادمة من الأقمار الصناعية لكوريا الجنوبية. وكان أطول هجوم على نظام جي.بي.إس نفذته كوريا الشمالية في 2012 واستمر لستة عشر يوماً، مسبباً اضطراباً في عمل 1106 طائرات و254 سفينة. بفضل قانون مور، تصبح تقانة إشارات جي.بي.إس أصغر وأرخص وأكثر فاعلية. وبالنتيجة، ليست القوات المسلحة وحدها من يستطيع الحصول على أجهزة التشويش الملاحية، بل بات أي شخص قادراً على ذلك. وسيكون لذلك آثاره المميزة على شاشاتك.

بالرغم من عدم قانونيتها في الولايات المتحدة الأميركية، فأجهزة التشويش نظام جي.بي.إس متوفرة بكثرة على الإنترنت في مواقع مثل www.jammer-store.com.، فمقابل 50 دولاراً فقط، يمكن لأي شخص أن يشتري نموذجاً خاصاً بلوحة عدادات المركبة يمكن إدخاله في مكان ولاعة السجائر الموجودة في المركبة ليخلق فقاعة مغنطيسية كهربائية تغلفك وأنت تقود سيارتك. واستخدام هذه النماذج شائع جداً لدرجة لا يمكنك تخيلها. إذ تقوم الشركات على نحوٍ متزايد بوضع وحدات نظام الموقع الجغرافي في كافة المركبات العاملة ضمن قوافلها التجارية. ويساعد ذلك شركات النقل لمسافاتٍ بعيدة وشركات التوزيع وأقسام الشرطة ومجموعات مركبات الأجرة وشركات المركبات المصفحة، ومزودي الكابلات على تعقّب الموظفين وإدارة العمليات وزيادة فعالية الوقود وتحديد إنتاجية العاملين. أما بالنسبة للعمال الذين يقودون هذه المركبات، فإن إضافة نظام جي.بي.إس يجعلهم يشعرون وكأن أخاهم الأكبر يراقبهم طوال الوقت. واستجابة لذلك، بدأ الموظفون بتخريب الأجهزة بقطع الأسلاك أو بإزالتها بشكلٍ كامل، ما كان يضعهم في ورطةٍ مع أصحاب عملهم بالطبع. أما الآن، فإن جهاز تشويش تبلغ قيمته 50 دولاراً يقوم بالحيلة نفسها دون أن يترك دليلاً

وراءه.

تكمن المشكلة في أجهزة التشويش المتنقلة هذه، في أن مفعولها قد يمتد ليصل إلى خمسمئة قدم حول المركبات التي تستخدمها. هذا يعني أن كل سائق مركبة لا يريد أن يراه رئيسه وهو يهمل عمله، يسبب التشويش على أنظمة جي.بي.إس لخمسين إلى مئة مركبة وفقاً لطاقة الجهاز. ولكن برنامج الملاحة في هاتفك أو سيارتك هو في الواقع أقل الشبكات المعرضة للتشويش بتلك الأجهزة أهمية. فكما رأينا في حادثة سان دييغو، وحتى لو لم يكن الأمر واضحاً منذ البداية، فإن أبراج الهواتف الخلوية وشبكات الطاقة والتحكم بالملاحة الجوية والصرافات الآلية، كلها تعتمد على نظام الموقع الجغرافي المبيّت فيها لتعمل بشكلٍ صحيح. وعندما يقرر سائقو الشاحنات الخروج من الشبكة، فإنهم يأخذون معهم خدماتٍ وأناساً آخرين، وقد تم تسجيل المئات من الحوادث مع أضرارٍ مباشرة سنوياً على هذا. ففي لندن، كان المضاربون يلاحظون أن مداولاتهم التجارية لا يتم إنجازها لمدة عشر دقائق يومياً، بسبب مشكلة في آلية الختم الزمني في النظام. وتساءل موظفو سوق الأسهم المرتبكون في ما إذا كانوا يتعرضون لنوع من الهجوم الإلكتروني من قوى أجنبية. لكن الأمر لم يكن كذلك، بل كان السبب هو سائق المركبة الذي أوقف سيارته بالقرب من سوق الأسهم، عندما كان يقوم بعمليات تسليم البضائع مرة كل يوم ولمدة عشر دقائق.

ليست حادثة التشويش التي جرت في لندن سوى واحدة من العديد من الأمثلة العالمية. ففي نيوجيرسي، قامت الحكومة بتنصيب نظام للمساعدة على الهبوط في مطار نيوارك ليبرتي، مزود بتقنية جي.بي.إس، للسماح للطائرات بالهبوط في حالات انخفاض مستوى الرؤية. ولأسبابٍ مجهولة، كان النظام يتوقف عن العمل مرتين في اليوم مسبباً لمراكز التحكم بالملاحة الجوية ارتباكاً أثناء إرشاد الطائرات القادمة. وبعد أن استمرت الحال لعدة

أشهر، اكتشف المسؤولون أن مصدر التشويش لم يكن سوى سائق مركبة يسير على الطريق الرئيسي في مدينة نيوجرسي، مستخدماً جهاز التشويش الموثوق على نظام جي.بي.إس، ليتجنب دفع الرسوم على بوابة المدينة (ومعطلاً أيضاً عمل شاشات التحكم بالملاحة الجوية في الوقت نفسه). وثمة بلا شك استخدامات إجرامية لأجهزة التشويش على نظام جي.بي.إس لا تقف عند مجرد تجنب دفع الرسوم على بوابة نيوجرسي. فبعد تعرضها عدة مرات لحملات بوليسية مفاجئة، تعلمت عصابات الجريمة المنظمة، بل وحتى عصابات الأزقة، أنه في حال ذهابك لسرقة سيارة، وخاصة تلك التي تحمل حمولة قيمة بما فيه الكفاية، بحيث يكون منطقياً وجود جهاز تعقب فيها، فمن الأفضل لك أن تتحضر وتمهد طريق الفرار باستخدام جهاز تشويش على نظام جي.بي.إس، وهو ما يقومون به بالفعل. لاحظت قوات الشرطة في الولايات المتحدة الأميركية وألمانيا وروسيا وإنكلترا أن المركبات المسروقة التي كانت تطاردها كانت تختفي فجأة عن الرادارات عندما يشغل المجرمون أجهزة التشويش على نظام جي.بي.إس، التي توفر لهم فقاعة وقائية يشقون بحمايتها طريق الفرار. وفي أحد الحوادث في المملكة المتحدة، نجحت عصابة جريمة منظمة في استخدام أجهزة التشويش على نظام جي.بي.إس لسرقة أكثر من أربعين مقطورة ضخمة، بحمولة تتجاوز قيمتها 10 ملايين دولار.

إذا ما اعتبرنا مستوى التشويش الذي تحدثه أجهزة تشويش صغيرة، فتخيّل ما يمكن أن تفعله الأجهزة الأكبر حجماً. فبتكلفة تقدر ببضعة آلافٍ من الدولارات، تتوفر للبيع على الإنترنت بكثرة أجهزة تجارية للتشويش على الترددات الراديوية. وسيكون نشر جهاز أو جهازين من هذا النوع حول منطقة مدنية كفيلاً بخلق تشويش واسع، يجعل من المنطقة صيداً ثميناً لأية منظمة إرهابية تحاول أن تلفت انتباه العالم. وكانت جدية هذا

التهديد كافية لجعل الحكومة الأميركية تُصدر تحذيراً مخيفاً جاء كما يلي: "لا بد من تطوير وإسراء سياسة تشمل عدة وكالات حكومية فوراً للتصدي للنمو المخيف في وفرة أجهزة التشويش على نظام جي.بي.إس... قد يكون التهديد الذي يحيق بأمننا القومي مدمراً".

ثمة بالطبع خطر يتهدد نظام الملاحة العالمي أخبث من مجرد منع وصول الإشارات إلى شاشتك، وهو تغيير الإشارات قبل وصولها. إذ لا يتوقف عمل أجهزة التشويش على حجب إشارات المواقع فحسب، بل يمكن للمشوشين أيضاً أن يبدلوا بيانات المواقع التي تتلقاها. وقد أصبحت المكيدة الشريرة التي صُوّرت في فيلم الغد لا يموت أبداً المنتج عام 1997 حقيقة مع توفر أجهزة تزوير إشارات جي.بي.إس بكثرة على الإنترنت، وهي تسمح لأولئك الذين تتوفر لديهم الوسائل والطاقة التقنية بأن يبثوا إشارات جي.بي.إس أرضية مزيفة خاصة بهم. ونتيجة للطبيعة الضعيفة لإشارات جي.بي.إس، يقوم مزورو الإشارة بخداع أجهزة الملاحة عن طريق التغطية على الإشارة الحقيقية بواحدة أخرى مزورة أقوى. وحالما يتم إنجاز ذلك، يمكن للمجرمين والقراصنة والإرهابيين والحكومات السيطرة على أي جهاز استقبال وربطه بجهاز محاكٍ متدني التكلفة، قادر على توليد الإشارات المقابلة للطريق المطلوب على خريطة غوغل إيرث. وهكذا، يمكن لإرسال إشارات كاذبة أن يقود ناقلة بترول إلى جسر أو قافلة عسكرية إلى منطقة العدو. وإذا أخذنا في اعتبارنا الإذعان اللاشعوري لسائق المركبة اتجاه أجهزة جي.بي.إس، فما مدى الخراب الذي يمكن أن يحدثه هجوم تزوير إشارات شامل على السائقين في مدينةٍ ضخمة؟

حدثت هجمات تزوير إشارات جي.بي.إس في العديد من المناسبات في أنحاء العالم حتى الآن. ولنفكر بأثر ذلك على صناعة واحدة فقط هي الشحن العالمي للبضائع. فوفقاً للمنظمة العالمية لأمن شحن البضائع،

تتكبد الشركات 25 مليار دولار سنوياً جراء سرقة الحمولات، التي يجري نقل 90 بالمئة منها عبر بحار العالم. ونظام جي.بي.إس هو عنصر لا بد منه لضمان وصول البضائع الصحيحة إلى المكان الصحيح في الوقت المناسب. ومع ذلك فإن أنظمة التزوير الملاحي قادرة على إحداث صدعٍ كبير في الدرع الذي يحمي هذا النظام. إذ تعتمد جميع سفن المسافرين والبضائع في البحار (والتي يبلغ عددها 400,000 سفينة في العالم تقريباً) على نظام تحديد الهوية الآلي، لإعطاء موقعها للسفن الأخرى ولسلطات الميناء التي يمكنها رؤية جميع المراكب المجاورة في الزمن الحقيقي. إلا أن بحثاً أمنياً أثبت عام 2013 أن نظام تحديد الهوية الآلي يفتقر إلى أبسط الضوابط الأمنية، وأنه قد يقع ضحية هجمات تزوير إشارة ستكون فضائحية. فمن شأن هجوم على هذه الأنظمة أن يؤدي إلى اختفاء ناقلات النفط وسفن السفر عن مجال الرؤية أو اصطدامها بعضها ببعض أو جنوحها إلى البر. ولأن أنظمة المواقع الجغرافية والملاحة هي "مرافق خفية"، فإننا نميل نحو نسيانها، ولكننا نخاطر بأنفسنا بفعل ذلك. وفيما لا يزال الموقع الدقيق للطائرة التابعة للخطوط الماليزية MH370 لغزاً، حين كتابة هذه السطور على الأقل، فإن شيئاً واحداً يبقى واضحاً. لقد كانت أنظمة الملاحة المسؤولة عن تتبع حركة الطائرة غير مؤهلة تماماً لأداء هذه المهمة. الموقع مهم، والمعلومات الملاحية الضعيفة أو الغائبة أو غير دقيقة قد تكلف البشر حياتهم.

سبق أن أدركنا أثر التشويش على أنظمة المواقع الجغرافية عندما نتذكر حادثة عام 2013، حيث تم خطف يخت تبلغ قيمته 80 مليون دولار عن طريق تزوير إشارات نظام الموقع الجغرافي. وكان اليخت الفخم البالغ طوله خمسة وستين متراً واسمه White Rose of Drachs يبحر قرابة السواحل الإيطالية، عندما بدأ فجأة بالاتجاه نحو اليمين. كان القارب في

البحر المتوسط في رحلةٍ من موناكو إلى رودوس عندما أطلق القراصنة جهاز تزوير الإشارات ذا الصندوق الأزرق. فوجهوا جهازهم الذي يعادل بحجمه محفظة اليد نحو أنظمة الملاحة الخاصة بالسفينة، حيث بدأ ببطءٍ ومن دون أن يلاحظ يرسل إشارات موقع مزورة. في البداية، كانت قوة الجهاز اللاسلكي الزائف ضعيفة بشكلٍ مُتعمّد. وبالتدريج بدأ رنينه يزداد، إلى أن بدأ يكافئ الإشارات الحقيقية المُسْتَقبلة من قبل السفينة، ثم ما لبث أن هيمن على تلك الإشارات. والآن أحكم القراصنة سيطرتهم على اليخت بشكلٍ كامل وأصبح بإمكانهم توجيهه كيفما يشاؤون. أما في قمرة القيادة، فلم تُقرع أجراس الإنذار وظل القبطان على اعتقاده الخطأ بأنه لا يزال يتحكم بسفينته.

لم يكن من الممكن تمييز الإشارات الزائفة للقراصنة من تلك الحقيقية، ما مكنهم من إنجاز مهمتهم. وبالرغم من أن أولئك الموجودين على سطح المركب ربما لاحظوا أن اليخت قد قام بتغيير واضح في اتجاهه، فإن الشاشات المسؤولة عن الملاحة في قمرة القيادة كانت تُظهر أن القارب يسير بالاتجاه الصحيح. لقد أصبح هجوم تزوير الإشارات في عرض البحر الآن أمراً واقعاً. ولحسن حظ الركاب وطاقم السفينة، فإن الخطف لم ينفذه قراصنة صوماليون بل طالبان متخرجان من جامعة تكساس، هما جاشان بهاتي وكين بيسينا. وكان الاثنان يعملان مع البروفيسور تود هيمفريس الذي عبّر ولسنوات عديدة عن قلقه حيال انعدام الأمن في نظام الموقع الجغرافي وحيال اتكالنا عليه.

تماماً كما برع المجرمون في استخدام أجهزة تزوير نظام الموقع الجغرافي ليسهّلوا سرقاتهم ويؤمنوا طرق فرارهم، لا شك في أنهم سيستغلون هذه الأجهزة لتضليل عربات نقل البضائع الكبيرة وتوجيهها نحو نقاط التسليم الخطأ، بل استدراج سفن الشحن إلى المراسي الخطأ لترسو فيها بينما تقبع في

انتظارها عصابات مجرمة بزي الموظفين سيسعدها تفريغ كافة البضائع والسلع في حاوياتها. فوحدة نظام موقع مشوّشة تكافئ عملية سطو ناجحة باستخدام السلاح. وإذا كانت الفكرة تبدو غير مألوفة، فتذكر قانون مور وجهاز آيفون في جيبك. فالتقانات التي تصبح أصغر وأسرع وأرخص تنتهي إلى أيدي المجرمين حتى قبل أن تصبح شائعة الاستخدام بين العامة. وبالسيطرة على شاشات الملاحة للسفن في البحر وعربات الشحن ومركبات المسافرين وحتى الطائرات، يمكن للقراصنة أن يصمموا واقعاً مزوراً لا يمكن تمييزه عن الحقيقة يسمح لهم بسيطرةٍ غير مسبوقة على عالمٍ تديره الشيفرات الحاسوبية وشاشات من كافة الأشكال والأحجام.

يمكن التلاعب بإيماننا الراسخ بالشاشات بطرقٍ جديدة ومبتكرة أيضاً، وحتّى بتزوير البيانات الخاصة بالمواقع التي نراها على تطبيقات هواتفنا الذكية. ففي بداية عام 2014، قام طلاب في المعهد الإسرائيلي للتكنولوجيا بقرصنة تطبيق ويز فائق الشعبية للملاحة باستخدام جي.بي.إس (والذي اشتراه غوغل عام 2013 مقابل مبلغ لا بأس به بلغ مليار دولار). والتطبيق الذي يوفر خدمة إدارة حركة المرور بالزمن الحقيقي بواسطة التعهيد الجماهيري، يعتمد على المستخدمين الذين يسجلون الحوادث ونقاط تفتيش الشرطة ومخاطر الطرقات كوسيلةٍ لتحسين سير المركبات على الطرق. وحالما يتم تشغيل التطبيق على هاتفك، فإنه يستخدم قراءات نظام جي.بي.إس على جهازك لتسجيل مدى سرعة المركبة، ويرسل هذه المعلومات إلى شبكة ويز ليوفر تقارير استخبارية لحظة بلحظة عن حالة الازدحام في المدينة. يعمل التطبيق بشكلٍ رائع عادةً، وهو يحافظ على سلامة وحياة الناس في المدن المزدحمة جداً (كما يؤكد الثمن الذي دفعته غوغل). لكن شاشات ويز، كغيرها من الشاشات، عرضة للوقوع في قبضة القراصنة.

سجل الطلاب في المعهد الإسرائيلي مجموعة من مستخدمي ويز المزيفين في النظام، مستخدمين برنامج توليد شيفرات مؤتمتاً قاموا بتطويره لانتحال شخصية الآلاف من الهواتف الذكية (وهو هجوم يعتمد على استخدام ما يشبه دمى الجورب). وفي ما بعد قام هؤلاء المستخدمون الافتراضيون للهواتف الذكية بالاتصال بتطبيق آخر يولّد مواقع مزيفة على نظام ويز، ما جعل جميع المستخدمين يظهرون وكأنهم يتحركون بشكل طبيعي في المدينة. وأخيراً، قامت الدمى عمداً بعرض آلاف التقارير التي "تزعم أنها عالقة في ازدحام مروري في المواقع المزيفة التي تدعي وجودها فيها". وقام نظام ويز بالنتيجة بما هو متوقع تماماً، حيث أعاد توجيه الآلاف من المستخدمين الحقيقيين بعيداً من الازدحام المروري المزعوم، مسبباً اختناقاً مرورياً حقيقياً في المدينة، فيما كان السائقون الغافلون يتدفقون معاً إلى الطرق التي كانت لتوها لا تعاني ازدحاماً مرورياً. يمكن لهذه التكتيكات، حين تنفّذ على نطاق واسع، أن تسبب المزيد من الذعر والفوضى لدعم أي هجومٍ إجرامي أو إرهابي آخر.

عندما يهاجم الجنرال تسو

فيما يعتبره المحققون حملة "منسقة وخفية ومستهدِفة للتجسس الإلكتروني ضد شركات غربية كبرى مختصة في مجال الطاقة"، قام القراصنة الصينيون وفقاً للتقارير بسرقة "غيغابايتات من الوثائق الحساسة الداخلية، من بينها معلومات تجارية عن عمليات التنقيب في حقول الغاز والنفط وتمويل المشاريع ووثائق المناقصات". واستخدم المجرمون تقنياتٍ متنوعة، لكن إجراءات الحماية القوية المستخدمة لدى بعض الشركات النفطية كانت بين الحين والآخر كانت تشكل تحدياً للصينيين. ولا تقتصر طريقتهم التكتيكية الذكية على استهداف ضحيتهم بقوة أكبر، بل تعمل أيضاً على جعل الضحية تأتي إليهم بنفسها عبر ما يُعرف باسم "هجوم

الحفرة المائية". وتم إطلاق هذه التسمية اعتماداً على مناورة مشابهة كانت استخدمتها الأسود في سهول سيرينغتي لآلاف السنين، وتقوم هذه الاستراتيجية على تواري المفترسين في حفرة مائية تأتي إليها الحيوانات العاشبة. وعندما تصل الحمير الوحشية والظباء والغزلان، تقفز الأسود لتقتل الفريسة الظمأى. أما الهجوم المكافئ على الإنترنت فيعتمد على تفخيخ موقع إلكتروني تزوره الضحية باستمرار. فما إن يقوم المستخدم الساذج بزيارة الموقع والنقر على رابط أو تحميل ملف معين، حتى يكون المفترس قد أحكم قبضته على الفريسة. ويبقى السؤال الوحيد المطروح هو أية مواقع يجب تفخيخها؟

عبر مراقبة نشاطات الهدف المقصود على الإنترنت (وعادة ما يكون شركة نفط أميركية ما)، توصل القراصنة إلى الكشف عن نموذج تكراري. فقد كانت أهدافهم تحب طلب الطعام من مطعمٍ قريبٍ جداً من المكتب الرئيسي لشركة الطاقة العملاقة، وهو مطعم صيني مشهور بطبق الدجاج اللذيذ والمعروف باسم جنرال تسو. لذا، يقوم القراصنة باستهداف لائحة الطعام الخاصة بالمطعم الصيني على الإنترنت بفيروس، وبينما كان العمال يستعرضون قائمة الطعام، كانوا "يقومون ومن دون قصد بتحميل شيفرة برمجية تمنح المهاجمين موطئ قدم في شبكة الحواسب الواسعة للشركة". إن استخدام الحكومة الصينية لقائمة طلب للطعام لإعادة إحياء قوة واحدٍ من أعنف جنرالاتها، هي فكرة مبهرة وهستيرية وتهكمية في آن معاً. وستكون سعيداً عندما تعلم أن وانغ باودونغ، المتحدث باسم السفارة الصينية في واشنطن، حين سُئل عن هذه الحادثة، جاء جوابه بأن "المزاعم التي أثيرت حول القرصنة الصينية غير عادلة"، وأن "لدى الصين قوانين صارمة ضد نشاطات القرصنة، كما أنها هي نفسها ضحية لمثل هذه النشاطات". أتساءل كيف كان الجنرال تسو سيجد ما قاله السيد وانغ.

اللعب بالشاشات: قرصنة البنية التحتية في سبيل المرح والتخريب

جميع البيانات الظاهرة على الشاشات هي عرضة للقرصنة، لا فقط المعلومات الموجودة على الحواسب النقالة وأجهزة آيباد أو حتى قوائم الطعام الصينية. وبدءاً من شاشات العرض الكبيرة التي قد نجدها في مباراة لفريق ليكرز وصولاً إلى الأضواء البراقة وآلات تسجيل الأخبار في ساحة التايمز، تتكاثر الشاشات، وكل واحدة منها عرضة للتلاعب، بما في ذلك شاشات تلفزيوناتنا. ففي عام 2013، تمكن القراصنة من التحكم بنظام الطوارئ في ولاية مونتانا وأطلقوا إنذاراً على قناة كي.آر.تي.في، شريكة سي.بي.إس. ففي ذلك العصر، استُوقِف بث البرامج التلفزيوني المسائي فجأةً بثلاثة أصوات فرقعة تنبيهية تلتها نغمة نظام الطوارئ القومي الخافتة، وهو ما يعني تحذيراً من كارثةٍ على وشك الوقوع عادة ما تكون شيئاً مثل زلازل أو إعصار. إلا أن التحذير الذي جاء في مونتانا نبه الناس إلى أن "السلطات المدنية القائمة على منطقتكم تحذر من أن جثث الموتى تنبعث من القبور وتهاجم الأحياء". وحذّر المعلِن المشؤوم "لا تحاولوا الاقتراب أو إلقاء القبض على هذه الجثث، لأنها تُعتبر خطيرةً للغاية". وبعد أن اتصل العشرات من المدنيين المرعوبين بمكتب الشريف المحلي، اعترفت المحطة أن ذلك الإنذار لم يكن يخصها، فقد تعرضت آلية تغذية الأخبار في المحطة للقرصنة، وتمكن أحدهم من السيطرة على موجات البث التي تصل إلى شاشتك بعيداً من محطة سي.بي.إس.

حتّى إشارات المرور اليومية باتت لعبة سهلة بأيدي القراصنة. ففي روسيا، استطاع القرصان إيغور بلينيكوف التحكم بشاشةٍ من نوعٍ آخر هي عبارة عن لوحةٍ إلكترونية إعلانية ضخمة، يبلغ أبعادها عشرين وثلاثين إنشاً كانت في أحد الشوارع العامة في موسكو، حيث سيطر عليها في ساعة الذروة. فمن بيته الذي يبعد سبعمئة ميل، قام بلينيكوف بالوصول إلى

مخدم وكالة الإعلانات التي تمتلك النسبة الساحقة من الإعلانات واستبدل ملفات الفيديو الإعلانية الخاصة بها عن الفودكا والأزياء بأخرى إباحية فاضحة. ونتيجة لذلك، "توقفت الحركة المرورية توقفاً تاماً عندما أراد السائقون إلقاء نظرةٍ على مقطع الفيديو الإباحي الجنسي الذي وضعه القراصنة على اللوحةٍ الإعلانية الضخمة" في طريق غاردين رينغ، الذي صادف أن يكون قريباً من وزارة الداخلية. ومن نافل القول إن السلطات لم تجد ذلك مسلياً، فقد تلقى بلينيكوف حكماً بالسجن لمدة ستة أعوام.

يتم الاستيلاء على شاشات الإعلانات العامة وبشكلٍ متزايد لعرض رسائل سياسية أيضاً، بل رسائل عنصرية أيضاً. ففي ذروة التوتر بعد حادثة إطلاق النار على تريفون مارتن في ولاية فلوريدا عام 2012، كانت النفوس تغلي في أنحاء البلاد. ومع تلك الخلفية، اختار أحدهم اختراق نظام تشغيل لوحةٍ إعلانية رقمية موجودة على الطريق إنيرستيت 94 في ديربورن بولاية ميتشيغن، ليغير الرسالة المعروضة عليها لتصبح "تريفون زنجي". بقيت العبارة على الشاشة يتفرج عليها المارة على الطريق السريع المزدحم لأكثر من ساعةٍ إلى أن تمكن العمال من إيقاف الجهاز وإعادة تشغيله. من شأن مثل هذه الرسائل التحريضية أن تدفع الوضع المتوتر أصلاً إلى الهاوية. وقد يسبب القراصنة الاضطراب أو الذعر أو الغضب عن طريق التلاعب بما نشاهده على شاشاتنا وتلفزيوناتنا ولوحات الإعلانات التي تحيط بنا.

إن قرصنة الإشارات الطرقية وإذاعات الطوارئ وإشارات نظام الموقع الجغرافي هو أمر مقلق، لأن تلك الأشياء تمثل جزءاً من البُنى التحتية المعلوماتية الحساسة: "هذه العناصر الجوهرية للمجتمع المتحضر التي من شأن تدميرها أو إضعافها أن يترك أثراً موهناً على الأمن القومي والاقتصاد والصحة العامة وسلامة المجتمع". وتمثل وزارة الداخلية أحد هذه القطاعات التي تضمّ أيضاً الطاقة والغذاء والزراعة والرعاية الصحية

والنفط والغاز والمياه والنقل، وخدمات الطوارئ والدفاع والخدمات المالية وصناعات النقل. ومع ذلك فالشيء الوحيد الذي تشترك به كافة تلك القطاعات الخدمية الهامة هو الاعتماد شبه التام على تكنولوجيا الحواسب والشاشات كعناصر أساسية لضمان عملها على نحو سليم وآمن. وكما سبق أن رأينا في المنشأة النووية الإيرانية في ناتانز، يمكن بسهولة لمثل هذه الأنظمة أن تتعرض للتهديد والهجوم. وتبقى هذه الحقيقة هامة بالنسبة لمعظم المواطنين في كلٍّ من العالمين المتقدم والنامي.

ربما كانت التهديدات التي يتعرض لها أي قطاع من قطاعات البنية التحتية أكثر من أن يمكن ذكرها جميعاً هنا، لكن بعض الأمثلة من صناعة النقل وحدها ستكون كفيلة بتقديم درسٍ كافٍ. تقوم الشاشات بتنظيم حركة المركبات والسكك الحديدية والنقل البحري والتحكم بالحركة الجوية، ويبقى النظام عرضة للخطر في كل خطوةٍ على الطريق تقريباً. ولنأخذ على سبيل المثال النقل الجوي، فإذا كان هناك بند مزيف واحد حول أي مسافر في قاعدة بيانات مراقبة الإرهاب، فيمكن أن تغير الطائرة وجهتها في منتصف الرحلة لتقوم بهبوط طارئ أو تتلقى مرافقة من قبل مقاتلات إف 16. وحتّى الإجراءات الأمنية التي تطبق عند الصعود إلى الطائرة تعتمد بشكلٍ كبير على الشاشات، إذ لا يقوم موظفو الأمن بتفتيش كل مسافر وفتح كل حقيبة، بل يتركون الأمر للتكنولوجيا لتقوم بالعمليات المرهقة، فتتولى آلات أشعة إكس أمر الأمتعة المتحركة على شريط النقل، بينما يوكل أمر المسافرين إلى عدد متنوع من كاشفات المعادن وماسحات الموجات الميليمترية والماسحات الجسدية. إلا أن ما يميز هذه الإجراءات الأمنية هو وجود طبقة من التكنولوجيا تتوسط بين موظفي الأمن وما يحققون في أمره من أشياء وأشخاص، وهي فرصة سانحة للقراصنة ليقوموا بعملهم مع ما ينتج عنه من عواقب قد تكون قاتلة.

بالرغم من أن الماسحات الجسدية في المطار تبدو آلاتٍ معقدة ومتخصصة، فإن وظائف المعالجة الأساسية فيها ترتبط بحواسب شخصية عادية تشغّل برمجيات تعمل على نسخ اعتيادية من نظام ويندوز قابلة، كجميع الآلات التي تعمل بنظام ويندوز، للاختراق بسهولة. فحتى في عام 2014، كانت معظم هذه الأجهزة، ومنها الجهاز الواسع الانتشار رابيسكان 522B، تستخدم نظام ويندوز بتنويعاته المختلفة، مثل ويندوز 98 أو حتّى ويندوز إكس بي، وهي نظم تشغيل تم توثيق احتوائها على آلاف نقاط الضعف الأمنية إلى حدّ أن شركة مايكروسوفت نفسها توقفت عن إصدار تحديثات لهذه الأنظمة. إضافة إلى ذلك، عادة ما توصل مجموعات الماسحات في المطار بعضها البعض عبر شبكة تستخدم أسلاك إيثرنيت أو موجات الوايفاي، البروتوكولين اللذين لطالما تعرضا للاختراق. ومن دواعي الصدمة أن كلمات سر مشغلات العديد من أجهزة الكشف في المطارات تُحفظ "بتنسيق نصي بسيط، وثمة العديد من الطرق للدخول إلى النظام دون معرفةٍ مسبقة حتى بالأسماء الحقيقية للمستخدمين". وحتّى عندما يستخدم المهاجم حساب وكلمة سر مُختلقين تماماً، فإن نظام هذه الآلات سيعرض رسالة خطأ ليتيح بعد ذلك للمهاجم الدخول كما اكتشف الباحث الأمني بيلي ريوس من شركة كوالِس للأمن السايبري.

نظراً لعدد هجومات اليوم، صفر الممكن شنها ضد البرامج المشغلة لهذه الأنظمة والثغرات الأمنية التي تعانيها، فإنه إذا أصيب جهاز أشعة إكس في المطار لفيروس من روتكيت، لاستطاع القراصنة التحكم بشكلٍ كامل بالصور التي يشاهدها موظفو الأمن على شاشاتهم. وهكذا يمكن جعل حقيبة من نوع تومي تحتوي على قنبلة أو قطعة سلاح تظهر على الشاشة وكأنها حقيبة تومي تحتوي ثلاث بزّات وزوجَيْ أحذية من برونو ماغليس. تتوسط الشاشات بين موظفي الأمن ومهامهم، ما يجعلها عرضة لهجمات الرجل

الوسيط. ففي الوضع النموذجي لعمل الأمن المطار، يقوم موظف بمراقبة الحقائب الداخلة إلى الآلة، فيما يقوم موظف آخر بفحصها بأشعة إكس، وأخيراً يشرف موظف ثالث على إزالة الحقائب عند خروجها من الجهاز. ووفقاً لهذا التوزيع للمسؤوليات، يكون الموظفان الأول والثالث قادرين على رؤية حقيبة التومي أثناء دخولها وخروجها من الجهاز، فيما تقَدّم للمراقب الثاني صورة فيديو عن حقيبةٍ أخرى مختلفة تماماً. ولأن الشخص الموجود في الموقع الثاني نادراً ما يشاهد الحقيبة مباشرة، فإنه يعتمد كلياً على ما يقدمه الحاسب ليحدد ما إذا كانت الحقيبة قد عَبَرت الفحص الأمني أم لا.

عبر السيطرة على محطة تفتيش بالفيديو في المطار، يمكن للقراصنة تمرير الأسلحة دون أن يكتشف أمرهم. وبالرغم من أن إدارة أمن النقل قد تسارع إلى إنكار إمكانية حدوث ذلك، فإن بيلي ريوس وفريقه أثبتوا أن أجهزة مثل جهاز رابيسكان 522B تحتوي مسبقاً على ميّزة خاصة بالمشرفين تسمح لمسؤولي الإدارة بمراقبة العشرات من الآلات والتحكم بها في المطارات في أنحاء البلاد وبالزمن الحقيقي، وهي تسمح لهم بالتأثير على ما يشاهده المراقبون الأفراد على أجهزتهم. وباستخدام تكتيك شائع لدى القراصنة، تمكّن ريوس من تجاوز شاشات تسجيل الدخول في محطة شاشات المراقبة والسيطرة على مجموعات ماسحات أشعة إكس.

السؤال الطبيعي هنا هو، ما الهدف من ملاحقة أجهزة المطار التافهة التي تعمل بأشعة إكس إذا كان الهدف هو إحداث كارثة جوية كبيرة؟ تعتمد الأنظمة العالمية للتحكم بالملاحة الجوية بدورها على الشاشات، وقد سبق للقراصنة أن نجحوا في اختراقها في عدة مناسبات. فوفقاً للمفتش العام في وزارة النقل الأميركية، فإن "القراصنة قاموا باعتراض أنظمة التحكم بالملاحة الجوية في ألاسكا وأحكموا سيطرتهم على مخدمات شبكة وكالة

الطيران الفدرالية، وسرقوا معلوماتٍ شخصية تعود لـ 48000 موظف حالي وسابق في الوكالة، وقاموا بتنصيب شيفرة خبيثة على شبكات الملاحة الجوية". ولقد حذّر المفتش العام من "أن وكالة الطيران الفدرالية غير مجهزة بما فيه الكفاية لكشف عمليات التسلل إلى أنظمة حواسبها". كما أشار إلى أن "الوكالة لديها أجهزة كشف في إحدى عشرة منشأة فقط من منشآتها البالغ عددها 734 في أنحاء البلاد ككل". وعلاوةً على ذلك، فقد كشف الفحص الأمني لشبكات التحكم بالملاحة الجوية الخاصة بوكالة الطيران الفدرالية، 763 نقطة ضعف تقنية عالية الخطورة ضمن نظام الوكالة.

تنفق وكالة الطيران الفدرالية في الولايات المتحدة الأميركية مليارات الدولارات على تحديث نظام التحكم بالملاحة الجوية في البلاد. ويُدعى النظام الجديد، نظام الجيل القادم للنقل الجوي، أو نيكستجين، و"سوف يكون آلياً ويعتمد على نظام الموقع الجغرافي جي.بي.إس بدلاً من الرادار لتحديد موقع الطائرات". (نعم وهو نظام جي.بي.إس الحساس نفسه اتجاه هجمات التشويش والتزوير المنظمة الواسعة الانتشار). سيسمح النظام المطوّر لوكالة الطيران الفدرالية بتخديم عدد أكبر من الطائرات والمروحيات العمودية، وحتّى الطائرات من دون طيار التي تجوب السماء المكتظة، وذلك باستخدام شبكة بث للمراقبة الآلية وبعض شفرات الحاسب التي سترسل لها الطائرة، وباستمرار ترددات لاسلكية لتُعرّف عن هويتها وتحدد للعالم موقعها. ولسوء الحظ، فإن هذه الإشارات غير مشفّرة ولا تخضع لتحديد الهوية. لذا فإنها قد تتعرض للتزوير مسببة الفوضى على شاشات المتحكمين بالملاحة الجوية. فعندما يقوم القراصنة بإدخال مئة سرب من الطائرات الوهمية إلى شاشة المتحكم بالحركة الجوية، سوف يعمّ الذعر. وإذا استمرت الحيلة لمدة ساعة واحدة، فسوف تنتشر آثارها في

كافة أرجاء عالم الملاحة الجوية المدنية لتشل حركة الرحلات الجوية العالمية. والأسوأ من ذلك هو أن محللين يعملون في القوى الجوية، نشروا مادة في الصحيفة العالمية لحماية البنية التحتية الحساسة، حذروا من خلالها من أن العيوب في شبكة بث المراقبة الآلية "قد تسبب عواقب كارثية من بينها التشويش وهبوط الطائرات أو حتى تحطمها إذا تم استغلالها من الخصوم".

تمثل سيطرة القراصنة على شاشات الحركة الجوية في العالم أفقاً مستقبلياً مخيفاً بالفعل، ولكن حتّى قرصنة الشاشات العادية يمكن أن تؤدي إلى عواقب خطرة، مثل تلك القرصنات التي تستهدف صناديق الاقتراع. ففي عصرنا الحالي، حتى صناديق الاقتراع القديمة تحوّل نفسها إلى برامج إلكترونية وشاشات لمس. فمع أن عمليات تزوير الانتخابات ليست بالأمر الجديد (فقد حصل صدام حسين وكيم جونغ - يون نسبة 100 بالمئة من أصوات الناخبين باستخدام الاقتراع الورقي)، فإن الانتقال إلى الأنظمة الرقمية يخلق فرصاً جديدة، ليس فقط لقرصنة الحواسب بل لقرصنة الديمقراطية أيضاً. وهنالك عشرات التقارير عن أنظمة اقتراع إلكتروني يتم اختراقها في أنحاء العالم.

أراد المسؤولون في واشنطن العاصمة أن يُسهّلوا عملية التصويت للمواطنين، وخاصة الغائبين منهم، كالذين يؤدون الخدمة العسكرية حالياً. ولهذا السبب أنفقت المدينة مئات الآلاف من الدولارات على أنظمة الاقتراع الإلكترونية. وكان موظفو المقاطعة قلقين جداً من إمكانية حدوث تزوير لعمليات الاقتراع على الإنترنت. لذا، وقبل إطلاق نظامهم الجديد، وضعوه مباشرة على الإنترنت وتحدوا القراصنة ليروا ما إن كان بإمكانهم تحطيم نزاهة آليات الاقتراع على الإنترنت. وفي غضون ثمان وأربعين ساعة، استطاع باحثون من جامعة ميتشيغن السيطرة على مخدم لجنة الانتخابات

سيطرة كاملة. ولم يتمكنوا من تغيير الأصوات التي أتت إلى المخدم وحسب، بل استطاعوا رؤية كيفية تصويت كل ناخب، محدثين بذلك خرقاً في سرية نظام الاقتراع الذي يشكل الأساس الذي تقوم عليه الديمقراطية. بل إن التصويت لم يغلق بعد أن شق فريق ميتشيغن طريقه للوصول إلى آليات الاقتراع في المقاطعة. وانتخب بِندَر، الإنسان الآلي الخصم في مسلسل الخيال العلمي الشهير فيوتشراما، رئيساً لإدارة المدرسة وبأغلبيةٍ ساحقة. ولم يكن بِندَر قد ترشح في الواقع، ولكنّه كان المرشح الملحق الذي حصد أغلبية الأصوات.

من المثير أن فريق جامعة ميتشيغن، أثناء تجولهم في الحواسب التي هاجموها، التقوا قراصنة آخرين من إيران والهند والصين كانوا يحاولون تخريب النظام. وكضربة قاضية أو إهانة أخيرة يوجهونها لعالم الاقتراع على الإنترنت، قام القراصنة الشرهون بتغيير برنامج المقاطعة، بحيث كلما نقر الناخبون على زر الاقتراع تتم السيطرة على مكبرات صوت حواسبهم ويضطرون لسماع دوي كورس جامعة ميتشيغن وهو يغني أغنية "فايت". أما موظفو المقاطعة فلم يدركوا أن النظام قد تعرض للهجوم إلا بعد يومين من الاختراق، عندما قامت مواطنة عجوز بالاتصال بالبلدية لتخبرهم أنها وجدت العملية على الإنترنت أسهل من الذهاب إلى مكتب التصويت. وفقط عندما أخبرت موظفي المقاطعة كم استمتعت وهي تستمتع إلى الأغنية بعد أن صوتت، أدركت لجنة الانتخابات أنها تواجه مشكلة. وليست تجربة ولاية كولومبيا فريدة من نوعها، كما ليس الشك في نزاهة أنظمة الاقتراع الإلكترونية في أميركا وحول العالم بسر، بل هي سؤال محوري يمسّ الديمقراطية نفسها. فعندما تصبح أصوات الناخبين عبارة عن إلكتروناتٍ مُسجّلة في الحواسب، تسنح الفرصة للأشخاص الأشرار ليفرضوا سطوتهم.

والمشكلة في أنظمة الاقتراع وإدارة الملاحة الجوية على الشاشات هي أن تلك الأنظمة التي تشغل هذه البنى التحتية الحساسة غير آمنة أبداً. ونحن باستخدامنا هذه الأنظمة في حياتنا اليومية دون التفكير بالعواقب الواضحة جداً، نزداد اتصالاً واعتماداً وقابلية للخداع، ونضع أنفسنا بذلك في مخاطر كبيرة قد تؤدي إلى كوارث في المستقبل. نظراً إلى الفرص المتاحة لقرصنة البُنى التحتية المعلوماتية الحساسة لبلد ما، لا عجب في أن تلجأ الدول القومية إلى ذلك تحديداً كبديل للحرب أو الصراع المسلح.

السواتر الدخانية وفوضى الحرب

جميع الحروب تقوم على المكر.

سون تزو

منذ أيام سون تزو، كانت القوات العسكرية تعتمد على فن الخداع لكي تحقق تفوقاً تكتيكياً على الأعداء. ففي بلاد الإغريق القديمة، كانت هدية الحصان الخشبي الضخم التي قُدمت إلى أهالي طروادة مفتاح الخدعة. وأثناء الحرب العالمية الثانية، كان بث الراديو الزائف والدبابات البالونية القابلة للنفخ في عملية فورتيتيود (الثبات) هما ما أوهما بوجود هجوم للحلفاء على شواطئ كالايس (النورماندي سابقاً) وسمحا لجيوش الأميركيين والبريطانيين باستعادة القارة الأوروبية وهزيمة النازيين. ونظراً لكون الجنود يعيشون عالمهم اليوم عبر شاشات حواسبهم، فإنه من المنطق اعتبار تكنولوجيا المعلومات قد باتت أحدث ميدان للحرب. تحدد الشاشات لقادة المعركة مكان طائراتهم وسفنهن ودباباتهم وجيوشهم. وتنظم الشاشات اللوجستيات وعمليات التوريد، وتوفر أحدث المعلومات الاستخبارية عن خطط العدو وإمكاناته ونواياه. ولا عجب بالطبع في أن هذه الشاشات تتحول باطراد إلى أهداف مفضّلة عند محاولة خداع العدو أو هزيمته.

في التعاليم العسكرية الحديثة، ثمة أسماء عديدة لمثل هذه النشاطات، حيث يطلق عليها تارةً اسم عمليات المعلومات وتارةً الحرب الإلكترونية أو عمليات شبكة الحواسب، أو حرب المعلومات أو العمليات النفسية. ويكون الهدف الرئيسي من هذه العمليات هو "التأثير أو التشويش أو إفساد صناعة القرار لدى الخصوم أو الهيمنة عليها". وفي الماضي، كان ذلك يتم عن طريق نشر شائعاتٍ زائفة ومعلوماتٍ مضللة شفوياً لأحد الخصوم أو عن طريق إلقاء منشورات ورقية تحتوي معلومات كاذبة فوق المدن المأهولة. أما اليوم فأصبح كل شيء يعمل بالشاشات. وأنظمة الشاشات وتكنولوجيا المعلومات مناسبة جداً لعمليات الخداع. فالشيفرة الحاسوبية ضعيفة وسهلة التخريب، ما يجعل النظام ككل هشًّا. وهذه الأنظمة جميعها تقريباً متصلة بطريقةٍ أو بأخرى بشبكة معلومات عالمية، ما يسمح باختراقها من قبل أعداءٍ يبعدون آلاف الأميال. وفي النهاية، تشكل هذه التقنيات جزءاً من أي بنية تحتية حساسة لأي بلد، والاعتماد عليها يعني ضعف أية حكومة أو شعب عندما تتعرض هذه الأنظمة للهجوم أو الإضعاف.

بعض محاولات الخداع هذه مُبسّطة. ففي المعركة بين الحكومة السورية وقوات المتمردين، تعرض موقع تابع لوكالة أنباء رويترز للقرصنة، لينشر أخباراً زائفة مفادها أن الثوار تعرضوا لهزيمة فادحة في مدينة حلب، وهو ما لم يكن الواقع الحقيقي. وهنالك قنابل دخانية رقمية أخرى أكثر تطوراً، مثل نجاح جيش الدفاع الإسرائيلي في اختراق الرادارات العسكرية السورية قبل الهجوم على موقع نووي قيد الإنشاء في الشمال من سوريا. فتحت اسم عملية أورتشارد، نجحت الغارة الجوية في تدمير مفاعل نووي عسكري سري كان يُبنى بمساعدة الكوريين الشماليين. وكانت الغارة الإسرائيلية تتطلب التوغّل جوًّا داخل سوريا وصولاً إلى الحدود مع العراق تقريباً.

وللقيام بذلك دون افتعال حرب حقيقية وتعرض المقاتلات الإسرائيلية للإصابة، قام الإسرائيليون باختراق الدفاعات الجوية السورية، ونجحوا بخداع حكومة الأسد أثناء تنفيذ الهجوم. فمع أن مقاتلات العدو كانت في طريقها نحو هدفها في عمق الأراضي السورية، كان الوضع هادئاً وطبيعياً على شاشات القوى الجوية السورية. فقد كانت الشاشات على الأرض تنقل واقعاً مختلفاً عن ذاك الذي في السماء.

في عالم عمليات المعلومات يكثر اللاعبون. وقد يجد مهاجمو اليوم أنفسهم في موقع الضحية ذات يوم. وهو ما حدث أوج الصراع الإسرائيلي مع حركة حماس في قطاع غزة في يناير عام 2009. فقد كان التوتر يزداد حدة في كلٍ من إسرائيل وغزة. وعندما بدأ الإسرائيليون بحشد قواتهم في الجنوب تمهيداً لعملية اجتياح لقطاع غزة، كان المئات من جنود الاحتياط قد بدؤوا يتلقون رسائل "تزاف شمون"، أو مكالمة الطوارئ الخاصة بالخدمة العسكرية، عن طريق البريد الصوتي أو الرسائل النصية على هواتفهم النقالة. وبالفعل تم استدعاء الاحتياط وبدأت الأمور تصبح جدية بالنسبة لجميع الأطراف.

أُعطيت الأوامر للعديد من الجنود الإسرائيليين للحضور، على أية حال، لا إلى الجبهة على طول الحدود الجنوبية مع غزة، بل إلى أقصى شمال البلاد، في مركز التجنيد التابع للقوات الإسرائيلية في حيفا. وكما اتضح، كانت تلك الرسائل مزيفة مصدرها حركة حماس. ففي الوقت الذي كانت فيه إسرائيل بحاجة لحضور جنودها للخدمة بالقرب من غزة، تم تضليلهم وتوجيههم نحو الشمال، وذلك لأنهم اعتمدوا على التعليمات الصادرة عن شاشاتهم. أي فخر لك يا سون تزو! كانت كل من إسرائيل وحماس تنفذ حرباً نفسية إلكترونية إحداهما ضد الأخرى. وأعلنت حماس أنها كانت قادرة على إرسال سبعين ألف رسالة نصية في الساعة إلى الهواتف النقالة الإسرائيلية، ما يؤكد

أن الإمكانات التي تطورها دولٌ قومية قد تنتقل وبسرعة لأيدي أطراف غير حكومية ومنظماتٍ إرهابية مع الوقت.

وثمة طريقة أخرى تتبعها الحكومات والأطراف غير الحكومية للهيمنة على شاشاتك، وهي طريقة دمى الجوارب. هل تتذكر الحسابات المزيفة البالغ عددها 140 مليوناً على الفايسبوك؟ ليست جميعها مُعدة للاستخدام كإعجاباتٍ مزورة لشاكيرا. فكما اتضح، يلجأ الموظفون العسكريون والاستخباريون في أنحاء العالم إلى مواقع التواصل الاجتماعي سعياً منهم للخداع والتلاعب بما نشاهده على شاشاتنا. ولقد ذكرت التقارير أن الحكومة الأميركية تستخدم دمى الجوارب على نحوٍ واسع كجزءٍ من عملياتها النفسية في مواجهة "الأيديولوجية المتطرفة والشائعات". أي إن الأميركيين يراقبون المنتديات الجهادية على الإنترنت، وعندما يقول "عبد الله" "الموت للكفار" فإن البنتاغون قد يمتلك شخصاً افتراضياً يُدعى "حسان" في جعبته جاهزاً للاستجابة بآياتٍ من القرآن تُمجد السلام والرحمة والتسامح. وما هذه بالطبع سوى أبسط الإمكانات. والشخصيات المزورة قابلة للتوسع أيضاً، فبوجود الآلاف من الدمى تحت سيطرة المرء، تزداد أسّياً إمكانات التأثير والخداع.

في حزيران من عام 2011، تم الكشف عن أن مركز القيادة الأميركي منح عقداً بقيمة 2.76 مليون دولار لشركة في كاليفورنيا لإنتاج شخصيات مزورة على الإنترنت بهدف التلاعب بالمحادثات ونشر وجهات نظر مؤيدة للأميركيين على مواقع التواصل الاجتماعي. ووفقاً للعقد، كانت كل شخصية مزورة على الإنترنت تحتاج إلى تاريخ شخصي معقول، وأن ذلك "يعتمد على خمسين مُتَحكماً مقرهم في الولايات المتحدة... يكونون قادرين على تشغيل الشخصيات المزورة من محطات عملهم دون الخوف من أن يتم اكتشافهم من قبل الخصوم المحترفين". وكان الهدف العسكري هو إنشاء لوحة تحكم

بالشخصيات على الإنترنت، تسمح لكل جندي أو جندية بالتحكم بعشر شخصيات مستقلة موجودة حول العالم "لإضعاف رواية العدو". وبالحديث عن النمو الأسّي للقوة، كانت الدمى التي تم تشغيلها بالعربية والفارسية والباكستانية والأفغانية، تسمح للعاملي الأميركيين بالتلاعب بالمحادثات على الإنترنت على مدار الساعة كما يشاؤون. وكان عقد الدمى هذا جزءاً من عملية تحالف عسكرية كبيرة بلغت قيمتها 200 مليون دولار، وأطلق عليها تهكماً اسم عملية الصوت الجادّ، العملية التي ظهرت أولاً في العراق "كسلاحٍ في الحرب النفسية ضد ظهور مؤيدي القاعدة على الإنترنت... وضد الجهاديين عبر باكستان وأفغانستان والشرق الأوسط".

حين يتم إنشاء محرك الخداع الافتراضي الأسّي، تتوفر للقائمين على إدارته وتشغيله سلطة كبيرة لقمع المعارضة وإضعاف رواية أعدائهم. فالشيء الوحيد الذي يعوق استخدام هذه الوسيلة للقمع المحلي هو السياسة العامة والقانون، وكلاهما مطواع ومتغيّر. فوفقاً لمجلس الحرية، وهو منظمة عالمية غير حكومية أُسست عام 1941 للدفاع عن الديمقراطية وحقوق الإنسان، فإن ما لا يقل عن اثنتين وعشرين حكومة حول العالم تتلاعب بوسائل التواصل الاجتماعي لأهداف الدعاية ونشر الشائعات، ومن بين هذه الدول فنزويلا ومصر وماليزيا.

في روسيا، كشف تحقيق سري أجرته صحيفة سانت بيترسبورغ تايمز، أن العديد من المنظمات السرية الموجودة تستخدم شباباً يتمتعون بخبرة تقنية كـ "مشغّلين على الإنترنت" لنشر مواضيع وتعليقات مؤيدة للكرملين ولتشويه سمعة قادة المعارضة. ويحصل كل مشغل للإنترنت على 36 دولاراً تقريباً، مقابل مدة عمل تصل إلى ثماني ساعات يُنتَظَر منه خلالها أن يكتب ما لا يقل عن مئة مداخلة في اليوم. ويحظى الرئيس الروسي، فلاديمير بوتين، والذي كان مقدماً في البوليس السري زمن الاتحاد السوفييتي، بسمعة طيبة

في مجال الدعاية، فوفقاً للتقارير، فإنه يستخدم "جيشاً سرياً من المروّجين للدعاية على الوسائط الاجتماعية" ينشر حوالى أربعين ألف تعليق في اليوم لمصلحته. فحين تكتب الصحافة العالمية أو المحلية في روسيا سواءٌ عن حقوق الشواذ أو أحد مرشحي المعارضة، تنبري جيوش من الدمى لترد مباشرة رداً قوياً. وتقديراً للخدمة البارزة التي قدموها للأمة، وخاصة خلال عملية "تحرير" شبه جزيرة القرم، منح بوتين كثيراً من هؤلاء المشغّلين على الوسائط الاجتماعية "أوسمة خدمة الوطن".

لا يمكن بالطبع مقارنة العملية الروسية لصياغة ما يراه الناس على شاشاتهم بالمقدرات التي طورتها جمهورية الصين الشعبية. فوفقاً لوكالة أنباء بكين وتقارير وسائل إعلام حكومية، تشغّل الصين ما يقارب مليوني عامل في مجال الدعاية للمساعدة في صياغة الرأي العام على الإنترنت وإدارة عملية الرقابة الإلكترونية المحلية. ويُدفع لهؤلاء المعلقين مقابل "إغراق الوسائط الاجتماعية بمجموعة من الأخبار والأفكار التي ترضى عنها الدولة". وفي بداية عام 2013، قام رئيس قسم الدعاية الصينية لو وي، والذي يلقب رسمياً برئيس مكتب الدولة لمعلومات الإنترنت، بتوجيه مستخدمي الإنترنت التابعين له والبالغ عددهم 2.06 مليون، بإنشاء حسابات على الوسائط الاجتماعية مثل موقع ويبو، وهو موقع تدوين مصغر شبيه بتويتر، بغية نشر "طاقة إيجابية" والمساعدة في توجيه النقاشات المتعلقة بالمواضيع الحساسة "في اتجاه إيجابي". ويتلقى هؤلاء العمال أيضاً تدريباً على كيفية ضبط النقاشات على الإنترنت وتوجيه المحادثات بعيداً من المواضيع السياسية الحساسة بالإضافة إلى الشك في قيمة المفاهيم الغربية للديمقراطية.

إن فن دمى الجوارب الحكومي هو تتمة فعالة للرقابة الإلكترونية. وتضمن هذه الرقابة عدم تمكن العدد الأكبر من الأفكار غير المرغوب بها

من عبور جدار النار القومي، لكن إذا استطاعت ذلك بالفعل، فإن جيوشاً من الدمى يمكن إطلاقها سراً لتقوض أية فكرة لا تتناسب مع رغبة من هم في السلطة. وفي كلتا الحالتين، يتم التلاعب بالشاشات لضمان بقاء من هم في السلطة في مكانهم وعدم بروز أفكار جديدة تتحدى سلطتهم. فحروب أجهزة العرض تستعر في أنحاء العالم كل يوم مع تصارع الحكومات والشركات المتعددة الجنسيات والمجرمين والإرهابيين لصوغ ما يظهر على الإنترنت والتحكم به. وما يترتب على ذلك في الواقع هو حرب حقيقية، لكن سرية، غايتها إعماء أعيننا عن الحقيقة. ولعل المحزن هو أن الموقف يزداد سوءاً مع ظهور أجيال جديدة تتمتع بتقانات أكثر فعالية على الإنترنت، ما يفصلنا أكثر بعد عن معايشة الحقيقة التي ليس لها شكل واحد أو هيئة واحدة ناتجة عن توسّط شخص آخر.

كونترول + آلت + خداع

أحد تعريفات السلامة العقلية هو القدرة على التمييز بين الواقع والخيال. وسنحتاج قريباً إلى تعريف آخر.

ألفين توفلر

عام 1865، مرر الكونغرس قانوناً تشريعياً يسمح لمدير مصنع صك العملة الأميركي، بإضافة شعار "إنما ثقتنا بالله" إلى جميع العملات الذهبية والفضية التي يتم صكها للتداول. وأصبحت هذه العبارة، المشتقة في الأصل من المقطع الشعري الرابع للنشيد القومي للولايات المتحدة الأميركية، منذ ذلك الحين الشعار الرسمي للولايات المتحدة الأميركية. وفيما العديد من الأميركيين على المستوى الروحي لديهم قناعة عميقة بثقتهم بالله، فإن شيئاً ما قد تغير ومن منظورٍ عملي. فهم قد يذهبون إلى المعبد في كل ليلة من ليالي الجمعة أو إلى الكنيسة أيام الآحاد، لكنهم يتابعون شاشاتهم كل يوم. وكأننا انتقلنا إلى ثقافة "إنما إيماننا بالشاشات". فحين يكون هنالك شيء ما

على شاشة، سواء أكانت شاشة حاسب أو آيباد أو نظام تحكم صناعي أو إشارة مرور أو جهاز تحديد الموقع الجغرافي أو جهاز رادار أو هاتفنا النقال، فإننا نميل نحو الثقة بما نشاهده أمامنا. وقد شاهدنا مراراً وتكراراً وعلى أية حال كيف يمكن تزوير جميع الأشياء لخداعنا، بدءاً بأصدقائنا على الفايسبوك ووصولاً إلى الأرقام التي نطلبها على هواتفنا النقالة. فالمشكلة هي أننا نعيش حياة خاضعة تماماً لوساطة الشاشات وغيرها من التقانات، بالرغم من أنها تعطي مظهراً تملؤه الشفافية إلا أنها في الواقع تتم برمجتها وتشغيلها والتحكم بها من قبل الآخرين. ولا أحد منّا لديه أية فكرة عن كيفية عمل أي منها.

إننا نعيش وعلى نحوٍ متزايد في مجتمع "الصندوق الأسود"، المجتمع الذي تحدد فيه الصناديق السحرية الاتجاهات وتنقل الأخبار وتتداول بالأسهم التجارية وتقوم بالاتصالات الهاتفية وتقدم النصائح حول اختيار المطاعم وتضع معرفة العالم بين يدينا. أما كيفية عمل هذه التقانة الغامضة فيبقى أمراً مبهماً تماماً للمستخدم العادي. ففيما يسرّ معظمنا أنه لا يحتاج إلى معرفة تعقيدات كتابة الشيفرة الحاسوبية لكي يقوم باتصالٍ هاتفي أو يمر بالصراف الآلي أو استخدام نظام منع انغلاق المكابح في السيارة، فإن أولئك المتمكنين من هذه المعرفة يتمتعون بامتياز خاص يدفعهم نحو الأمام. وهم في موقع يسمح لهم بتحديد شكل العالم الذي ستعيش فيه الأعداد الكبيرة من الجماهير الخاضعة، التي تفضل ترك مثل هذه الأمور التقنية المزعجة لغيرها. وفي هذا العالم المتغير نسبياً الذي يحكمه قانون مور، يتمتع الخارجون على القانون، الخاضعون لقانون مور، بأفضلية كبرى.

كما نوهنا في الفصل الأول من هذا الكتاب، فإننا نصبح أكثر اتصالاً واعتماداً وحساسية اتجاه المخاطر كل يوم. فالأغلبية الساحقة من أنظمة المعلومات لدينا يمكن أن تُخْتَرَق في غضون دقائق، وهنالك نمو أسّي في عدد

الفيروسات وأحصنة طروادة وهجومات اليوم صفر، كلها متوفرة لمن يريد إتمام المهمة. أما الوقت الوسطي اللازم لاكتشاف الاختراق، أي بين اللحظة التي يقتحم فيها المتطفل النظام ولحظة فضح عملية القرصنة، فلا يقاس بالدقائق بل بمئات الأيام. ونحن نتعرض للاختراق والسبر الرقمي والتجسس والسرقة ويتم التلاعب بنا كل يوم عملياً، ويبقى معظمنا سعيداً بغفلته عن التهديدات. إنه العالم الجديد الذي صار اعتيادياً، حيث تكون كل شاشة في حياتك هدفاً لخطة هجوم لدى الحكومات أو المجرمين أو الإرهابيين أو النشطاء - القراصنة.

وفي النهاية، يمكن اختزال كل عمليات قرصنة الحواسب والتلاعب بالشيفرات وتبديل الشاشات إلى مسألة جوهرية واحدة هي الثقة. فالثقة تمثل صلب جميع هذه النقاشات، ولا يوجد في عالمنا في الوقت الحالي ما يمكن تسميته الحوسبة الموثوقة. فالأمن والخصوصية ومدى موثوقية التقانة، كلها جوانب من السهل التشويش عليها وتخريبها وتقويضها. والحقيقة هي أننا لا نملك فكرة ملموسة عما يجري داخل أنظمتنا، وهي الأنظمة نفسها التي نستخدمها يومياً بشكلٍ شخصي واحترافي وفي تشغيل العالم. وفيما نبقى بإخلاص على ثقتنا بالله، فإن رفع شعار الإيمان بالشاشات أمر مضلل وسيعود ليصيبنا بالضرر بطرق سوف نندم عليها.

تمثل ثغرة "القلب النازف" الأمنية التي خطفت الأضواء في بداية عام 2014 رمزاً للتحديات التي نواجهها. فالغاية من أنظمة التشفير الحاسوبية نظرياً، هي أن تعمل سرّياً على تشفير وفك تشفير المعلومات الحساسة التي يتبادلها طرفان. وأشهر بروتوكولات التشفير على الإنترنت هما طبقة المقابس الآمنة (إس.إس.إل) وأمن طبقة النقل (تي.إس.إل). والواقع هو أن نسخة من بروتوكول طبقة المقابس الآمنة، والمعروفة باسم إس.إس.إل المفتوحة، مسؤولة عن حماية أكثر من ثلثي الحركة على الإنترنت. وحتّى لو

كنت لا تعرف ما هو التشفير أو ما هو بروتوكول طبقة المقابس الآمنة، فإنه من الوارد أنك تستخدمها في كل مرةٍ تدخل فيها إلى حسابك المصرفي أو تتفقد بريدك الإلكتروني أو تشتري شيئاً عبر الإنترنت. فقد تدربنا على البحث عن إشارة القفل الأخضر الصغير التي تظهر على شريط عناوين محرك البحث على صفحات الإنترنت، وعلى البحث عن صفحات HTTPS بدلاً من HTTP لنضمن أن اتصالنا بموقعٍ معين آمن وموثوق. ويعني اللون الأخضر أنه بإمكانك المضي، فالوضع آمن وكل شيء على ما يرام، أو على الأقل هذا ما كنا نظنه.

كان الكشف الكبير الأساسي الذي تم عبر ثغرة القلب النازف، هو أنه بالرغم من أن الأقفال الصغيرة الخضراء على محركات البحث كانت تبين لنا أننا آمنون في بحثنا، فإن الحقيقة كانت عكس ذلك. والثقة التي وضعناها في أقفال بروتوكول إس.إس.إل المغلق على محركات البحث الظاهرة على شاشاتنا كانت في غير مكانها. لقد خانتنا "ثقتنا بالشاشات" مرة أخرى. فثغرة القلب النازف هي أضخم نقاط الضعف وأكثرها انتشاراً في تاريخ الإنترنت حتى الآن. مجرد خطأ برمجي في بروتوكول إس.إس.إل المفتوح جعل تلك المفاتيح السرية المشفرة، التي كنت تظن أنك تشاركها سراً مع مصرفك أو مع مخدمات شركات الوسائط الاجتماعية، مفتوحة فجأة أمام شخصٍ آخر. والأسوأ من ذلك بعد هو أن هذا العيب لم يكن قابلاً للكشف على الإطلاق، بالرغم من وجوده منذ شهر كانون الأول عام 2011. ما يعني أن جميع رسائل المحادثة والبريد الإلكتروني وعمليات الشراء على الإنترنت والمواقع التي تمت زيارتها والتطبيقات التي تم تحميلها خلال عدة سنوات خلت، كانت في الحقيقة متاحة تماماً لشخصٍ آخر لديه الوقت والقدرة والرغبة لفك شفرتها.

يُستخدم بروتوكول إس.إس.إل المفتوح من قبل 66 بالمئة من جميع

مواقع الويب على الإنترنت، ولهذا السبب كان على ملايين المواقع حول العالم أن تبلغ مستخدميها بوجود فجوة كبيرة تسمح للقراصنة بالالتفاف على نظام التشفير بينك وبين مواقعها. ومن بين الشركات التي تأثرت بهذه المشكلة إنستاغرام وبينتيريست وفايسبوك وتمبلر وغوغل وياهو! وإيستي وغودادي وفورسكوير وتوربوتاكس وفليكر ونيتفليكس ويوتيوب يو.إس.إيي.إيي ودروب بوكس وكثير غيرها. علاوةً على ذلك، فإن 150 مليون تطبيق محمّل على أجهزة أندرويد كانت في عداد الضحايا. وللأسف، فإن تغيير كلمة السر الخاصة بك لم يكن حلاً ناجعاً لهذه المشكلة من ناحية المستهلك. فكل موقع من هذه المواقع بحاجةٍ أولاً إلى تغيير برنامج مخدمه وتحديث نسخة إس.إس.إل المفتوحة التي يستخدمها، وإلا فإن أي مهاجم محتمل سيبقى قادراً على قراءة كلمة السر الجديدة الخاصة بك حتّى بعد تغييرها. وحتّى بعد شهرٍ كاملٍ من إعلان ثغرة القلب النازف، بقيت مئات آلاف المواقع تعاني الثغرة الكبيرة في العمود الفقري للتشفير الذي تعتمد عليه الإنترنت بمعظمها. أما المهاجمون، فلم يضيعوا وقتهم بالطبع وسارعوا لاستغلال الثغرة، وكان من بينهم وكالة الأمن القومي التي كانت تعلم بنقطة الضعف لسنوات، وفقاً للتقارير، ولكنها احتفظت بذلك لنفسها لكي تستغل الفرص المتاحة أمامها. وشارك المجرمون بدورهم في حمّى الذهب التي اندلعت بفضل ثغرة القلب النازف، فهاجموا وكالة العائدات الكندية (وهي تكافئ قسم الضرائب في كندا) وعشراتٍ من مواقع التجارة الإلكترونية حول العالم.

تُعتبر مفاتيح التشفير والرخص الرقمية الأدوات التي يتم عن طريقها توفير الحماية والأمان لبياناتنا الإلكترونية وما يتبعها من تقنيات. لكن ثغرة القلب النازف لم تكن المرة الأولى التي تعرضت فيها هذه الأنظمة للتخريب. فبشكلٍ عام، لا تتوفر بين أيدينا الأدوات التي تجعل عالمنا

التقاني آمناً وموثوقاً. لذا فإنه ليست لدينا الوسائل التي نحتاج إليها كمجتمعٍ عالمي لاتخاذ قراراتٍ ذكية وموثوقة في عالم يزداد اضطراباً. فالبشر لا يقرأون مباشرة الآحاد والأصفار على لوحاتهم، ونحن لا نفكر بالشفرة الثنائية (على الأقل حتّى الآن)، بل نستخدم مجموعة من الشاشات والآلات الأخرى لتفسّر لنا هذه المعلومات. ونحن بذلك نضحي بأي أملٍ حقيقيّ لفهم الحقيقة العميقة لأي شيء. وطالما كان بإمكان الآخرين التوسط بيننا وبين تجاربنا الرقمية والافتراضية، فسنبقى فريسة سهلة للخداع والاستغلال والهجوم، وليس هذا أساساً يمكن أن نبني عليه حضارة المستقبل.

ليس أكبر التحديات التي نواجهها في عالم "الثقة بالشاشات" متمثلاً في مشاكل اليوم، بل في تلك التي ستأتي غداً. ونظراً للآثار الواضحة لقانون مور، فإن عدد الشاشات الموجودة في حياتنا اليوم سوف يغدو تافهاً حين يقارن بما هو آتٍ. ولنستذكر هنا جملة مغني الراب نوتورتوس بي.آي.جي "شاشات أكثر، مشاكل أكثر". ستصبح الشاشات موجودة في كل مكان، على معاصمنا ونظاراتنا وعدساتنا وفي ملابسنا، فما تُسمى الشاشات القابلة للارتداء تزداد انتشاراً. وفي منازلنا، ستتحول طاولات غرفة الطعام وإطارات الصور والثلاجات والغسالات إلى العمل بالشاشات. وبينما نسافر من مكان إلى آخر لقضاء أعمالنا اليومية، ستكون الشاشات موجودة في مركباتنا وقطاراتنا وعلى مسند رأس كل مقعدٍ في الطائرة. ولائحات الطعام في المطاعم والمرايا في غرفة السيدات والجدران فوق المباول في حمامات الرجال، ستمطرنا جميعها بمعلوماتٍ مرئية. وليست لوحات الإعلانات هي وحدها التي ستتحول إلى شاشات، بل كذلك الجدران في المنازل وأبنية المكاتب والمحالّ. وستسود الخوذ المزودة بشاشات كتلك التي يستخدمها الطيار في طائرته الحربية أو المستخدمة في الواقع المعزّز، لتنتج طبقاتٍ وطبقاتٍ من المعلومات المرئية في شريط الرؤية الذي توفره لتؤثر إلى الأبد

في وجهة نظرنا. بل إن كل طبقة مسطحة محتملة ستتحول إلى شاشة تفاعلية، وستكون كل منها بمثابة فلتر ينتقي من واقعنا الذي يسهل التلاعب به من قبل أولئك الذين سمحنا لهم بتفسير العالم الحقيقي من أجلنا.

ثمة أشباحٌ في الأسلاك والشاشات ومصارف البيانات في عالم القرن الحادي والعشرين. ومع هيمنة العالم الرقمي والافتراضي على العالم الحقيقي، سنعيش حياتنا معتمدين على وساطة الآخرين، لكن ما هو ثمن ذلك؟ فشبكة المعلومات العالمية التي نتصل بها ونعتمد عليها على نحو متزايد هشّة للغاية.

ثمة عاصفة على وشك الهبوب، وجميع علامات الكارثة باتت موجودة. وحجر الأساس التقاني الذي نبني عليه مستقبل الإنسانية متزعزع جداً وهو أشبه ببيت من ورق قد يتداعى في أية لحظة. وبالرغم من ذلك، فإننا نتابع تقدمنا ونتبنى تقانات أحدث وأكثر تألقاً، كل منها يعد بحل مشكلةٍ جديدة أو بتقديم وسائل راحة معيّنة. ولا تكمن المشكلة في كون التقانة سيئة بحد ذاتها، فالعلم والتقانة يبشران في الحقيقة بفائدة عميقة تعود على الإنسانية. بل المشكلة، كما رأينا، هي أن أولئك الذين يملكون معرفة تقانية، سواء أكانوا مجرمين أم إرهابيين أم حكوماتٍ مارقة، ربما يستخدمون تفوقهم لاستغلال شريحة من العامة، تتوسع أسّياً بدورها، في غير مصلحتنا. وبالرغم من أن تقانات اليوم كانت نعمة على الأطراف غير الشرعية، فإنها ستبدو تافهة بالمقارنة مع مدى وعمق التغيير التقاني الذي سيتكشف لنا بسرعةٍ خلال السنوات القادمة. وثمة عدد وافر من التقانات التي لا تزال في بدايتها الآن سيصبح قريباً بين أيدينا، كالروبوتيات والذكاء الصنعي والتصنيع الثلاثي الأبعاد والبيولوجيا التركيبية، وستصاحب هذه التقانات فرص كبيرة للأذى من شأنها أن تغير حياتنا.

ربما استفاد المجرمون من الأدوات التقنية المتوفرة أمامهم حتى الآن، إلا أن الأسوأ لم يأت بعد. فقد أعدّت الحوسبة الهشّة غير الموثوقة ميدان المعركة لعالم مستقبلي يعجّ بالإجرام ويتّسم بانعدام الأمن الاجتماعي. إنه هدوء ما قبل العاصفة، ومن الوارد جداً أن ننتهي إلى قَدَر لم نتحضر له جيداً. إنه مستقبل الجريمة يرحب بكم.

الجزء الثاني

مستقبل الجريمة

الفصل العاشر
شركة الجريمة

تحقق الجريمة المنظمة في أميركا دخلاً يتجاوز الأربعين مليار دولار سنوياً... بينما لا تنفق سوى القليل على المستلزمات المكتبية.

وودي آلين

كانت شركة إنّوفيتف ماركتنغ شركةً ناشئة صغيرة وواعدة تنتج منتجات برمجية رائدة تلبي حاجات زبائنها. وقد قام مؤسسو الشركة الشبان بترخيصها في بيليز نظراً لأنظمتها الضريبية المشجّعة، في حركةٍ ذكية استقوها من الممارسات التجارية لعمالقة التقانة العريقين، مثل أبل وغوغل وإتش.بي، التي قامت كلٌّ منها بتأسيس شركاتٍ فرعية في الملاجئ الضريبية في أنحاء العالم. ولخفض التكاليف الزائدة أكثر بعد، قررت الشركة وضع مكاتبها الرئيسية في كييف بأوكرانيا، التي يكثر فيها خريجو الجامعات التقانيّة ذوو التأهيل العالي بدرجاتٍ متقدمة في علم الحاسب والرياضيات، وحيث يمكن تشغيل الموظفين برواتب لا تشكل إلا جزءاً ضئيلاً من الرواتب التي تقدم في وادي السيليكون.

كما تفعل أي شركةٍ ناشئة جيدة في مجال التقانة، كانت شركة إنّوفيتف ماركتنغ تروّج لمنتجاتها عبر الويب بواسطة اللوحات الإعلانية، وكانت تدفع المال لضمان ظهور برمجياتها على رأس قوائم البحث. ولكي تجتذب زبائن جدداً، لجأت الشركة إلى تقنيةٍ ناجعة ومجربّة قامت بتطويرها أمازون تعرف بتقنية التسويق بالمشاركة، فحين ينقر زبونٌ محتمل على رابطٍ مُستضاف تدفع الشركة لموقع الويب المُضيف رسوماً زهيدة مقابل تقديمه للإعلان، أما إذا تحققت مبيعاتٌ حقيقية بالفعل فإنّ المستضيف يتلقى رسوماً مئوية متفقاً عليها، وهو نظامٌ يأتي بعوائد على الجميع: فهو يشجع تعهيد الأعمال ويعطي الدفع لمبيعات البرمجيات للشركة الناشئة.

أحسن مؤسسا الشركة، شايلشكومر "سام" جن المولود في الهند والسويدي بيورن سُندِن، تنظيم خط بيع المنتجات البرمجيّة، فقد قرر الاثنان تركيز طاقتهما الإبداعية على تصميم صنفٍ جديدٍ كلياً من مضاد الفيروسات وبرمجيات الأمن الحاسوبي. وكان ذلك عام 2006 حين كان قلق العالم من التهديدات السايبرية يتصاعد، وكانت الأعمال تزدهرُ حينها ومبيعات الشركات من منتجات مثل برامج مكافحة البرمجيات الخبيثة ونظم الدفاع عن نظام التشغيل وبرمجيات مكافحة برامج التجسس على الويندوز، تتنامى عاماً بعد عام. وسرعان ما صارت الطلبات على منتجات الشركة تتدفق بالمئات ثم بالآلاف فبالملايين على مكاتب الشركة في كييف.

كانت شركة إنّوفيتف ماركتنغ، على غرار الكثير من الشركات الناشئة الناجحة الأخرى، تتلقى عدداً من الطلبات لا يمكنها تلبيته، وكانت تكافح لمواكبة هذا التوسع السريع. ولم يمرّ وقتٌ طويل حتى باتت الشركة تحتل ثلاثة طوابقٍ في بناء مكاتب حديث في الرقم 160 من شارع سيفيرو سيريتسكايا، في القطاع الصناعي المتنامي في كييف. أما في الداخل، فكان العشرات من المهووسين بالحاسب من ذوي المواهب المميزة يضخّون الشيفرات البرمجية بوتيرةٍ محمومة، بينما كان المهندسون يمدّون عناقيد من كابلات الإنترنت الجديدة ويضيفون أسراباً من المخدمات الحاسوبية سعياً لمواكبة طلبات الزبائن.

وفي رواق المركز الرئيسي المتوسّع للشركة، قام العمال بتعليق شعار الشركة الزجاجي الملون بقياس خمس أقدام على الجدار، ووراء نُضض موظفي الاستقبال المشغولين بالردّ على الهواتف وتحية الموظفين الذين كانوا يبدأون عملهم. ووراء منطقة الاستقبال الغارقة في الحداثة، كان الموظفون التنفيذيون يجدّون في تخطيط الإجراءات التجارية وفي وضع النظم في أماكنها لتأمين بنيةٍ تنظيمية لا بدّ منها لنمو الشركة. وراحت الأقسام تُضاف

قسماً تلو الآخر، من قسم تطوير البرمجيات إلى قسم ضمان الجودة والقسم المالي وقسم الفواتير وقسم التسويق وقسم الموارد البشرية وقسم الترجمة وقسم مَحلَلَة البرمجيات والأبحاث والتطوير والإنتاج والتعهيد الخارجي والدعم الفني. وكان جين وسوندن، كأيّ أبوين فخورين، يراقبان طفلهما وهو ينمو.

خلال مدةٍ وجيزة، تحولت شركة إنّوفيتف ماركتنغ إلى قصة نجاحٍ هائل، إذ أصبحت شركةً عالمية متعددة اللغات تعمل على مدار الساعة ويعمل فيها أكثر من 600 موظف ولديها زبائن في ستين بلداً. ومن خلال فروعها، قامت بتعهيد وظائف مركز مكالمات الدعم إلى الهند، للاستجابة لأسئلة الدعم الفني وخدمة الزبائن بالإنكليزية. أما متحدثو الألمانية فكانوا يتلقون الإجابة على أسئلتهم من العاملين المتمكنين من اللغتين في بولندا، بينما كان يتم تحويل الزبائن الفرانكفونيين عبر تقنية "الصوت عبر الإنترنت" إلى الجزائر. وكانت جميع مبيعات الشركة من البرمجيات مؤتمتةً وموزعةً على الشبكة، فكان بإمكان الزبائن شراء منتجاتهم بنقرةٍ من الفأرة بينما كان يتم توليد الأرقام التسلسلية للمنتجات عبر إيصالات ترسل بالبريد الإلكتروني، تقدم كفالاتٍ تضمن إعادة المال على البضائع المبيعة. وكانت الشركة تتعامل جدياً مع خدمة الزبائن، وكانت تنبه زبائنها الذين يتصلون بأرقامها الثمانمئة إلى أنّ المكالمات تخضع للرقابة لأسباب تتعلق بضمان الجودة. وتشير الإحصاءات التي كانت مراكز المكالمات تحتفظ بها، إلى أن أكثر من 95 بالمئة من الزبائن كانوا يعتبرون أنفسهم "سعداء" بالخدمة التي كانوا يتلقونها. وعلى غرار جميع الشركات الناشئة في مجال التقانة، كان لشركة إنّوفيتف ماركتنغ حضورٌ جيد على الوسائط الاجتماعية. فكان المئات من موظفيها قد أنشأوا حساباتٍ على موقع لينكدإن تتضمن مواقعهم في العمل وتاريخهم المهني. ولاجتذاب المواهب التي تتطلبها

تنمية الشركة الناشئة، كانت شركة إنّوفيتف ماركتنغ تضع إعلانات وظائف على الكثير من مواقع الويب المتخصصة بفرص العمل، وكانت تكلّف وسطاء توظيف بمساعدتها على إيجاد مديري المشاريع ومديري أنظمة يونيكس، والمتخصصين في أَمْثَلة محركات البحث والباحثين ومهندسي الدعم ومساعدي التطوير التجاري. وللتعامل مع نموها الانفجاري لجأت الشركة إلى العديد من التقنيات لمعالجة مسائل الموارد البشرية، التي عادةً ما تظهر في عالم الشركات الناشئة. فكانت تقدم الجوائز لأفضل مسؤولي المبيعات وتنتقي بعنايةٍ موظفيها كل شهر.

للتخفيف من الضغط الناتج عن وتيرة العمل المحمومة، كانت الشركة تكافئ موظفيها برحلاتٍ تنظمها لهم إلى مرافق ساحلية ينخرط فيها الموظفون في تمارين تساعد على بناء روح الفريق، كسباقات الجري وتسلق الجدران وتمارين الحبل ولُعب كرات الألوان بهدف رفع الروح المعنوية وتشجيع التعاون. وكيفما نظرنا إلى الأمر، كانت شركة إنّوفيتف ماركتنغ مكاناً رائعاً للعمل وشركةً رابحةً على نحوٍ مدهش. أما من وجهة نظر الزبائن فكان ثمة مشكلةٌ صغيرة. فقد كان من الشائع أن يحدث ما يلي: بينما يجلس المستخدم أمام لوحة مفاتيحه لينشر شيئاً على الفايسبوك أو ليردّ على بريد إلكتروني أو ليتفقد التقارير الرُبعية الأخيرة، تظهر فجأةً شاشة منبثقة كبيرة حمراء في وسط الشاشة قائلةً: تحذير: تم اكتشاف فيروسٍ خطير. وفي الوقت نفسه، تبدأ مكبرات صوت الحاسب بالعويل كصفارات إنذارٍ تقول للمستخدم إنّ شيئاً خطيراً جداً يحدث في نظامه. بعد ذلك بقليل يظهر شعار برنامج الدفاع عن النظام إلى جانب مُكبرةٍ ضخمة تبدو وكأنها تمسح ملفات القرص الصلب للمستخدم. ثم تظهر أسماءُ ملفاتٍ طويلة ومعقدة ملفاً تلو الآخر في تتابعٍ سريع، بينما يتم عرض عدد متزايد من تهديدات البرمجيات الخبيثة الجاري اكتشافها على شاشة نتائج

أسفل الشاشة. وفي النهاية قد يعرض برنامج الدفاع عن النظام ثلاثةً وعشرين فيروساً معروفاً وسبعة فيروساتٍ دُودية وثماني عشرة برمجية تجسس، إضافةً إلى تحذيرٍ يدعو إلى الذعر: "حاسبك مهدد تماماً بانهيار النظام وفقدان البيانات إلى الأبد. انقر هنا لإزالة جميع التهديدات".

بينما تستمر صفارات الإنذار بالصراخ في الخلفية من مكبرات صوت الحاسب، كان المستخدمون عموماً يختارون رد الفعل الأكثر بديهية عبر النقر على زر "إزالة التهديدات" المُتاح أمامهم. وكان يتمّ عندها تحويلهم إلى صفحة شراءٍ لبرنامج الدفاع عن النظام التابع لشركة إنّوفيتف ماركتنغ، وهو برنامجٌ بكلفة 49 دولاراً يضمنُ حل جميع المشكلات الحاسوبية المعروفة. أما أولئك الذين اختاروا بسذاجةٍ تجاهل خيار "إزالة التهديدات" وحاولوا النقر في أيّ مكانٍ آخر على الشاشة، فسرعان ما كانوا يكتشفون أن حاسبهم قد أُقفل تماماً فيما عدا صوت صفارة الإنذار البغيضة. فلم يكن مفتاح الهروب يعمل، ليبقي المستخدمون عالقين مع شاشةٍ حمراء ميتة غير قادرين على التحكم بحواسبهم. أما المستخدمون العارفون الذين اعتقدوا أنّ إعادة تشغيل الحاسب قد تحلّ المشكلة، فلم يجدوا أمامهم حين فعلوا ذلك سوى صفارة الإنذار نفسها المُزعجة والشاشة الحمراء الجامدة نفسها. وكان الحل الوحيد لاستعادة التحكم بالحواسب والبيانات هو دفع الرسوم البالغة 49 دولاراً (وكانت ثمة نسخة ممتازة مع دعم فني غير محدود بكلفة 79 دولاراً).

فما الذي قامت شركة المنتجات البرمجية الرائدة هذه بخلقه تماماً؟ كانت تلك برمجيةً إجرامية، وهي فئة منتجاتٍ جديدة تماماً في صناعة البرمجيات تشتمل على برمجيات ترتكب الجرائم. والبرمجيات المجرمة، التي تدعى أحياناً ببرمجيات الرعب وبرمجيات الفدية ومضادات الفيروسات المارقة، ما هي إلا برنامج حاسوبي خبيث يتلاعب بخوف المستخدم من الإصابة

بفيروس. فقد تمّ تدريبنا جميعاً على الانتباه إلى تحذيرات مضادات الفيروسات وعلى تشغيل برمجياتنا الأمنية حين نكتشف مشكلةً ما. فكان من المنطقي تماماً حين ظهرت رسالة النظام الحرجة الخاصة ببرنامج الدفاع عن النظام على شاشات المستخدمين في أنحاء العالم، أن يكون رد الفعل الأفضل والأكثر بداهةً هو النقر على "إزالة جميع التهديدات". لكن كانت ثمة مشكلةٌ صغيرة: فرسائل التحذير التي تمّ عرضها لم تكن سوى خدعةٍ برمجية مُتقنة تمثّل حالةً جديدة نخطئ فيها عندما "نؤمن بالشاشة".

لم يكن زبائن شركة إنّوفيتف ماركتنغ قد أصيبوا بفيروسٍ في الحقيقة على الإطلاق، بل كانت متصفحاتهم ونظم تشغيلهم قد تعرضت للخطف. أما الصورة الرسومية المتحركة التي أوهمت المستخدم بأن حاسبه يخضع للفحص بحثاً عن فيروسات، فلم تكن سوى حيلةٍ بصريّة لا تختلف عن فيلمٍ كرتوني من ديزني. ولم يكن أي حاسب يخضع للمسح على الإطلاق، والفيروسات وأحصنة طروادة التي تمّ "العثور عليها" لم تكن سوى اختلاقاتٍ افتراضية اخترعها البرنامج وعرضها على نحوٍ مقنع على الشاشة. وبعد أن يتم استدراج المستخدمين للدفع لقاء منتج حماية النظام وتحميله، تقوم البرمجية بأداء مهمتها الرئيسية الوحيدة: إزالة مضاد الفيروسات القانوني الموجود لدى المستخدم للسماح بإضافة المزيد من البرمجيات الخبيثة والأبواب الخلفية وبرمجيات تسجيل ضربات المفاتيح وتنصيبها على الأقراص الصلبة المُصابة. والأسوأ من ذلك أن البطاقات الائتمانيّة التي استخدمت لشراء البرمجيات الملغومة قد أصبحت الآن معروضةً للبيع بالمزاد في السوق السوداء. أما شركة إنّوفيتف ماركتنغ، بجميع ما لديها من مراكز مكالمات ومكاتب مشرقة وعوامل جذب للموظفين، فلم تعد سوى جبهةٍ في غاية النجاح للجريمة المنظمة الحديثة.

تمكنت إنّوفيتف ماركتنغ من خلق هذه السوق الهائلة لمنتجاتها الخبيثة

عبر استغلال فرق موظفيها وفرق العاملين لدى شركائها، لاستغفال مواقع الويب القانونية بواسطة إعلاناتٍ تجارية مصابة ببرمجيات خبيثة تنشرها شركاتها الفرعية. فحين كان مستخدمٌ غافلٌ يزورُ ببراءةٍ موقعاً مصاباً أو ينقر على الرابط الخطأ، كان يتم تحميل شيفرة برمجيةٍ خبيثة لإصابة جهازه، ما كان يسمح للمبرمجين في إنّوفيتف ماركتنغ بالوصول إلى ما يحتاجون إليه ليشرعّوا النوافذ الحمراء المقنعة. وفي نهاية المطاف، وبعد أن تقدم كثيرٌ من الزبائن بشكواهم إلى السلطات في عشرات البلدان، تمّ اكتشاف أمر المؤسسة الإجرامية وجاءت نتائج التحقيقات صادمةً. إذ كانت الشركة تحتفظ بنسخٍ لجميع الإيصالات التي أصدرتها في مكاتبها لمصلحة زبائنها الذين اشتروا البرمجيات الإجرامية في أنحاء العالم. وفي عام 2009 فقط قامت بمعالجة 4.5 مليون طلب منفصل من الزبائن يبلغ متوسط مبيعات كل منها 35 دولاراً. ما يعني أن الشركة قد حققت عوائد بمقدار 180 مليون دولار عام 2009، متفوقةً بوضوح على تويتر الذي حقق بعد ذلك بعامين، أي عام 2011، 106 ملايين دولار. أما المجموع المثير للدهشة الذي حققته الشركة خلال ثلاثة أعوام، هي الفترة التي كانت تبيع فيها البرمجيات الإجرامية، فهو 500 ميلون دولار على شكل مبيعات عالمية.

وسرعان ما تكشّف أن مؤسِسَي الشركة قد اختارا وضع شركتهما في أوكرانيا، لا فقط لتوفر المواهب التقانية بتكلفةٍ زهيدة وحسب، بل لأن السلطات كانت مقتضبةً في أسئلتها ولأنه من السهل جداً شراء السلطة التنفيذية. ويعترف العمال اليافعون في الشركة مثل مكسيم البالغ من العمر 22 عاماً، والذي كان يعمل مبرمجاً لدى الشركة، بأنّ العلاوات المتكررة سهّلت عليهم تجاهل المضاعفات الأخلاقية لأعمال الشركة. "حين تكون في العشرينيات لا تفكر كثيراً في الأخلاقيات"، يضيف. أما مؤسسا الشركة، السيدان جين وسوندن، فهما مُتهمان نتيجة لنشاطاتهما ومطلوبان لكلٍ من مكتب

التحقيقات الفيدرالي والإنتربول. إلا انهما تمكنا من الهرب إلى ملاجئ آمنة قبل أن يتم القبض عليهما ولا يزال مكانهما غير معروف. مع مئات الملايين من الدولارات المكدّسة في حساباتٍ مصرفية سرية في أنحاء العالم، حقق متعهدا الإنترنت هذان ما يحلم به معظم متعهدي وادي السيليكون: خروجاً ناجحاً من شركةٍ ناشئة. ومع أنها لم تعد تعمل، فإنّ شركة إنّوفيتف ماركتنغ في كييف ربما تكون واحدةً من أكثر الأعمال الإجرامية التقانية ربحاً على الإطلاق. لكنها على كل الأحوال ليست الوحيدة، إذ تشير التقديرات إلى أنّ نحو 35 مليون حاسب شخصي في أنحاء العالم تصاب باستمرار بمضادات الفيروسات المارقة هذه كل شهر، لتضع 400 مليون دولار كل سنة في أيدي عصابات الجريمة السايبرية العالمية الأخرى، إنه عالم شركة الجريمة يُرحّب بنا.

السوبرانوات السايبرية

لطالما قرأت أن "الجريمة لا تنفع". لا تكن مغفلاً! فهذه أشياء للمغفلين قصيري البصر وليست لأمثالنا.

جيمس كانيي، في "ملائكة بوجوهٍ قذرة"

تمثّل الجريمة مجال أعمالٍ كبيراً، وتقدرّ الأمم المتحدة عوائد الجريمة المنظمة العابرة للدول بأكثر من تريليوني دولار في السنة. وتعود هذه الأموال من تجارة المخدرات وسرقة الملكيات الفكرية والإتجار بالبشر والبضائع المزورّة، وموادّ الأطفال الإباحية وانتحال الهوية وتهريب الحيوانات البريّة و... بالطبع، من الجريمة السايبرية. ويعتقد أن نسبة إجمالي الجريمة المنظمة إلى إجمالي الناتج المحلي العالمي، تبلغ نحو 15 إلى 2 بالمئة. ويمكن اعتبارها الشبكة الاجتماعية الأضخم والأقل شرعيّةً في العالم، وهي تعتمد على التدوير المستمر للبشر والبضائع المزوّرة عبر الكوكب على مدار الساعة. لدى معظمنا بفضل هوليوود تصوراتٌ عن أفراد العصابات

النموذجيين حين يتعلق الأمر بالجريمة المنظمة، كزعماء الرُعاع من أمثال توني سوبرانو وفيتو كورليوني وتوني مونتانا. إلا أن المجرمين الحديثين تجاوزوا إلى حد كبير البنى الهيكلية التي كانت تسمُ الماضي، وباتوا يتبنون شكل المنظمات التجارية الحديثة. فقد تمّ استبدال أفراد العصابة وزعمائها بمختلف مراتبهم بشبكاتٍ إجرامية دينامية محليّة تتلقى مهامّها من الخارج، تتجمع وتعيد تشكيل نفسها لاستغلال أية فرصةٍ غير شرعيةٍ ممكنة.

الأزمنة الحديثة تستدعي الجرائم الحديثة. لذا فإنّ خلفاء توني سوبرانوز في أنحاء العالم قاموا ببناء وتغذية قوة عملٍ إجرامية أكثر قوةً وانتشاراً وتحقيقاً للأرباح وكفاءةً تقانيةً. ولتحقيق ذلك، قامت عصابات الجريمة التقليدية، مثل كوزا نوسترا (أي المافيا الإيطالية)، وياكوزا اليابانية وترياتس الصينية، إضافةً إلى عصابات الغوغاء الروسية والنيجريّة، بافتتاح أقسام جريمةٍ سايبرية للاستفادة من الأرباح العالية القليلة المجازفة التي يتيحها لهم العالم المتواصل في أنحاء الكوكب. فالجريمة السايبرية لا تعرف الحدود وتوفر إمكانات عظيمة لإخفاء الهوية، وهي نادراً جداً ما تشهد ملاحقاتٍ، فهي ربما لا تحدث إلا في أقل من واحد بألف من واحد بالمئة من جميع الحالات.

أما التوجه الرئيسي الثاني الذي يسمُ الانفجار في الجريمة السايبرية المنظمة فهو احتراف القراصنة أنفسهم، فقد تغير أسلوب عملهم على نحوٍ كبير مقارنةً بالأيام الخوالي في الثمانينيات، حين كان معظم القراصنة يتسلون بنظمٍ حاسوبية من باب الفضول أو لإثبات قدرتهم التقنيّة. إذ لم يعد الاختراق شيئاً يقوم به مراهقون تملأ وجوههم البثور ينشرون الخراب من أقبية منازلهم حيث يعيشون مع أمهاتهم، فأكثر من 40 بالمئة من المجرمين الناشطين في مجال الجريمة السايبرية تزيد أعمارهم عن 35 عاماً.

فقد اكتشف القراصنة الأفراد منذ وقتٍ طويل أنه من الممكن الحصول على المال عبر اختراق التقانة، فظهر قراصنةٌ مجرمون مثل ألبرت غونزالس وكيفن بولزن. حيث أدركوا أنه من الممكن تحقيق دخلٍ لا بأس به عبر اختراق الأنظمة الحاسوبية للآخرين على نحوٍ غير شرعي. ومع الوقت، انتشرت الفكرة وسرعان ما بدأ القراصنة بتوحيد صفوفهم في أنحاء العالم في شبكاتٍ سريعة يتعاونون من خلالها ويتنافسون على الأرباح الإجرامية.

وأصبح الاختراق نشاطاً مالياً كاملاً، وحدث التحول من القرصنة كهواية إلى عصابات الاختراق الإجرامية الربحيّة. وتم تأسيس عصابات الجريمة السايبرية العابرة للقوميات، مثل شبكة الأعمال الروسية و"شادو كرو" وسوبرزوندا، إضافةً بالطبع إلى شركة إنّوفيتف ماركتنغ، للاستفادة من الطيف الواسع من الفرص الذي تتيحه جريمة الجيل التالي، وراحت الأعمال تزدهر. وكأنّ التهديد الذي يمثله القراصنة الأفراد الذين يسرقون البطاقات الائتمانية وعصابات المافيا التي تحطمّ رُكب ضحاياها لم تكن كافية، تعمل عصابات الجريمة المنظمة التقليدية اليوم على الاتحاد مع القراصنة الموهوبين ليوحدوا قواهم، في ما يعود على العامة وعلى الأعمال التجارية بنتائج كارثيّة. ومع أنّ ثمانين بالمئة من المخترقين كانوا تاريخياً أفراداً مستقلين، فإنّ العكس هو الصحيح اليوم. فوفقاً لدراسةٍ أجرتها شركة رانت عام 2014، فإن ثمانين بالمئة من القراصنة يعملون اليوم كجزءٍ من عصابة جريمةٍ منظمة.

تذكرني نتائج دراسة رانت بمشهدٍ عظيم من فيلم "صائدو الأرواح" من الثمانينيات، حين يتسلح بلموراي وهارولد راميس ودان أيكرويد بـ "أسلحة بروتونية" للتغلب على الأشباح الذين اجتاحوا مدينة نيويورك، وفي إحدى لقطات الفيلم يشير راميس إلى النجمين المرافقين له "ثمة شيءٌ هام نسيت أن أخبركما به... لا تقاطعا الدفقات الصادرة عن أسلحتكما..

سيكون ذلك سيئاً". وحين يسأل موراي "إلى أي حد؟" يجيب رامس "حاول تخيل الحياة كما تعرفها تتوقف فجأةً لينفجر كل جزيءٍ في جسدك بسرعة الضوء". وجاء رد موري الجاف: "حسناً إنّه أمرٌ سيّئ. شكراً على التنبيه الهام". فإذا استعرنا من موري ورامس، يمكننا القول بأنّ عوالمنا الشبكية تتلاقى وأن "الدفقات" الإجرامية تتقاطع لندخل الآن عصر الجريمة الرقمية العظيم. في مملكة الجريمة الرقمية الجديدة هذه ضمّ القراصنة ورجال العصابات على الطراز القديم قواهم ليشكلوا "كتيبة الموت" الحديثة، التي تركز على استغلال التقانة إلى أبعد حدٍ ممكن لزيادة سطوتها وأرباحها على حسابك وحسابي.

قد لا يكون الاستغلال الإجرامي للتقانة جديداً بحد ذاته، فحين كان معظم رجال الشرطة لا يزالون يسيرون على الأقدام أو يمتطون صهوات الخيل بدأ أفراد عصابات شيكاغو باستخدام السيارات للهرب، وحين كان عنصر الدورية الاعتيادي مسلحاً بمسدس ست طلقات كان جورج كيلي، الملقب بـ "البندقية الآليّة"، يستخدم أسلحةً آلية. وتجار المخدرات هم أولى الفئات السكانية الكبرى بعد الأطباء التي تستخدم أجهزة البيجر للاتصالات، كما توفرت لهم الهواتف النقالة قبل أن يستخدمها رجال الشرطة بوقتٍ طويل. تجعل التقانة الجريمة أكثر فعالية، لذا فإن المجرمين دائماً ما يكونون سباقين إلى تبني أي شيء تقني.

يظهر الخارجون على القانون خبرةً خاصةً في استخدام التقانات التي يخلقها الآخرون واستغلالها وتسخيرها لأهدافهم الخاصة، وهم لا ينفكون يبحثون عن فرصٍ جديدة. فما إن بدأت الهواتف الذكية المزودة بالإنترنت تشيع، حتى بدأت عصابات الجريمة المنظمة في المكسيك باستخدامها لأهدافها البحثية. فما الذي كانت تبحث فيه؟ ضحايا الخطف بالطبع. فحين كان المسؤولون التنفيذيون الأغنياء يحطّون في مطار مدينة المكسيك

الدولي، كانوا بمثابة وليمةٍ من ضحايا الاختطاف المحتملين تقدم للمجرمين، الذين كانوا يتساءلون عن الشركات التي ستدفع الفدية الكبرى (أي أكبر عائد استثمار لاستعادة موظفيها)، الأمر الذي كان في منتهى الصعوبة إلى أن ظهرت الهواتف الذكية.

كانت فرق الجريمة المنظمة المنتشرة في المطار تقبع في الحيز المخصص للقادمين، بالقرب من موقع تسلّم الحقائب حيث تصطف أرتالٌ من سائقي السيارات المتهندمين بانتظار زبائنهم المسافرين من رجال الأعمال، الذين استقدموا هؤلاء السائقين مسبقاً. وكان كل سائقٍ يحمل لوحةً كبيرةً تحمل اسم الشركة واسم المسافر المنتظر، مثل السيد سميث من شركة ميرك للمنتجات الدوائية أو السيدة جاكسون من شركة غولدمان ساكس. وكانت العصابات الإجرامية في المطار تستخدم المعلومات الموجودة على اللوحات التي يحملها السائقون للبحث باستخدام هواتفهم الذكية في غوغل عن الموظفين التنفيذيين، لتحديد مواقع هذه الشركات وقيمتها الصافية. وحين كانوا يجدون السمكة الكبرى، كان الخاطفون يقتربون ببساطة من السائق الذي يحمل اللوحة الأكثر ربحاً ويدفعون له المال لقاء اختفائه أو يجدون حلاً آخر معه. وكان سائق بديل من العصابة يحمل الشارة التي أخذها من السائق الأصلي ويقف بها بهدوء منتظراً زبونه. وهكذا يكون الفخ قد نُصِب ليسير المدير التنفيذي الذي وصل توًّا مباشرةً إلى أحضان السائق المُزيف، كل ذلك لأن اللوحة التي كان يحملها السائق قد تمّ اختراقها. وقد تمّ اختطاف العديد من المديرين التنفيذيين، كما قتل آخرون باستخدام تقنية البحث بواسطة الهاتف الذكي هذه.

أياً يكن شكل الابتكار التقاني، نجد المجرمين سباقين إلى تبنيه سواءٌ بالتخفي على شكل شركة إنترنت ناشئة أو باستغلال خدمات مثل هذه الشركات. فقد قامت امرأةٌ في المملكة المتحدة باستعارة صفحةٍ من تطبيق

أوبر المتخصص في مشاركة السيارات، والذي يصل السائقين بالمسافرين، لإنشاء خدمتها الخاصة لطلب السيارات بواسطة الرسائل القصيرة لتقدم سياراتٍ تستخدم في الهروب. فبعد أن استشعرت بوجود حاجةٍ في السوق لدى المجرمين الذين لا يملكون سيارات، أنشأت نيكول جيبسون من لندنديري خدمة "سائق للهروب يستدعى برسالةٍ نصيّة"، لتساعد اللصوص على الهروب بأمانٍ بالبضائع التي يسرقونها من البيوت والمتاجر على طول الحدود الإيرلنديّة. وفي سان فرانسيسكو بدأ بائعو المخدرات في حديقة دولورس باستخدام سكوير، وهو جهازٌ بلاستيكي أبيض صغير يتصل بهاتف الآيفون ويسمح لأي شخصٍ بتلقي المبالغ المالية عبر بطاقة الائتمان، ما يسمح لمن يريد تجنب التعامل بالمبالغ النقدية بتقاضي الأموال لقاء المخدرات والحشيش. وفي نيويورك لجأت المومسات، وقد سِأمن الكاميرات ورجال الحراس المبالغين في استجواباتهم في فنادق مانهاتن الأنيقة إلى موقع إير.بي.إن.بي لاستئجار الشقق من أجل مواعيدهن. حيث يقدمن أنفسهنّ كطالباتٍ أو سائحات، أما النيويوركيون الغافلون الذي يؤجرون شققهم، فلا علم لهم بأنّ أسرّتهم تستخدم للترويج عن العديد من الزبائن وممارسة طقوس العربدة. وتدعي إحدى خدمات الترفيه هذه أنها توفر "ثروةً" عبر استخدام الموقع. "إنّه أكثر رصانةً وأرخص بكثير من موقع وول دورف"، كما تقول بائعة هوى في الحادية والعشرين. فأياً تكن التقانة أو خدمة الإنترنت المتوفرة نجد المجرمين موجودين في المراحل المبكرة يبتكرون في تسخير الأدوات المستجدة لمصالحهم.

شركة الجريمة: المخطط التنظيمي

تقدم شركة إنّوفيتف ماركتنغ على موقعها على الويب في الصفحة الرئيسية، كما تفعل الكثير من الشركات على الإنترنت، أقسام "من نحن" و"أسئلة شائعة" لمساعدة زوارها. وحين ينقر المرء على رابط "من نحن"،

يقرأ أنّ "إنّوفيتف ماركتنغ تعمل جاهدةً على تطوير العديد من المنتجات التي تساعد المستخدمين على التأقلم مع التغيرات التي تفرضها التقانة". وما تلك إلا صياغةٌ من الصياغات الممكنة. فلو أنها كتبت "تعمل إنّوفيتف ماركتنغ بجِدٍّ لسرقة الناس في أنحاء العالم عبر إيهامهم بأنّ لديهم فيروساً، واستدراجهم لدفع 49 دولاراً لإزالة شيءٍ غير موجود"، لأقدم عددٌ أقل من الناس على شراء منتجاتها. فعلى الرغم من تكتم عصابات الجريمة المنظمة نفسها حيال بُناها الفعلية وممارساتها التجارية، فإنّ العديد من العمليات السرية ومصادر السلطة التنفيذية وشركات الاستخبارات السايبرية قد سلطت الضوء على ممارساتها التجارية وتنظميها، وهو ما سنقدمه في ما يلي.

من المفاجئ أن المخطط التنظيمي للشركة الإجرامية يبدو مألوفاً إلى حدٍ بعيد لأي شخص يعمل في مجال التجارة التقليدية، فهو يذكر ببيتر دروكر مع مزيجٍ من آخر ما توصلت إليه الأعمال التجارية من ممارسات تُدرسّ في وارتون أو في مدرسة الأعمال في هارفارد. وبينما تشتمل الأوساط السرّية الرقمية على عناصر لا يحركها الربح وحده، مثل النشطاء - القراصنة، فإنّ الجريمة المنظمة تهتم أولاً وقبل كل شيء بالمال أو بقيم الأسهم إذا صحّ التعبير. وتذهب هذه المؤسسات الإجرامية إلى أبعد حدٍ ممكن لتضمن استمراريتها، لذا فإنها تحصر وجودها في الملاجئ القانونية الآمنة. أي في تلك الأماكن التي تحكمها حكوماتٌ ضعيفة ونظم سياسية غير مستقرة وتكون قوات الشرطة فيها مستعدة لغضّ أبصارها، مقابل رسومٍ بالطبع. وداخل هذه العصابات الإجرامية ثمة أقسامٌ متخصصة بإدارة العمل وإدارة سلاسل التزويد، ورئاسة أقسام ومستشارون خارجيون ومنتجات تقدمها الفرق. ولفهم طاقة الشركة الإجرامية ومدى احترافيتها لا بد لنا أولاً وقبل كل شيء، من إلقاء نظرةٍ على المخطط التنظيمي لها لكي نتمكن من تفكيك

المنظمة الإجرامية الحديثة. ففيما يلي بعض الأدوار والمسؤوليات الأكثر شيوعاً كما تبين الأبحاث السريّة:

المدير التنفيذي

يتولى المدير التنفيذي في أية مؤسسة إجرامية مسؤولية اتخاذ القرارات ومراقبة العمليات. فهو، كما معظم المتعهدين التقليديين، من يأتي بـ "الفكرة الكبيرة" ويوفر نواة رأس المال المخصص لتحقيقها، وهو غالباً ما يكون "شخصيةً شعبية" تتمتع بصلاتٍ تربطها بعناصر أخرى في عالم الجريمة. وهو يؤدي دور الداعية الذي يجمع الفريق الصحيح من المجرمين لتنفيذ أية مهمة. وليس من الشائع أن يكون عارفاً بعالم التقانة بعمق، لكنه يكلف آخرين ممن يتمتعون بالمهارات البرمجية والقرصنية بتنفيذ رؤياه. ولا يتورط المدير التنفيذي الإجرامي بأية أعمال يومية قذرة أو هجومات سايبرية قد تؤدي إلى تعقبه. بل هو يحدد الأهداف والغايات التي يسعى إليها فريقه ويراقب توزيع الإيرادات الإجرامية خصوصاً في أوقات العلاوات. ويعتمد المدير التنفيذي على دعم فريقٍ قيادي يشتمل على مديرين تنفيذيين آخرين.

المدير المالي

يتتبع المدير المالي المؤشرات الأساسية للعصابة الإجرامية، بما فيها مقدار البرمجيات الإجرامية التي تم بيعها وعدد الحسابات التي تم اختراقها وأرصدتها، وهو يستخدم أدوات إدارة العمليات التجارية، بما فيها نظم التقارير المالية وقواعد البيانات، لمعالجة المستحقات (للمتعهدين الإجراميين) والمدفوعات المخصصة للعمالة الإجرامية. كما أنه يحافظ على شبكةٍ معقدة من العلاقات المالية السرية لممارسة غسيل الأموال، وهو مسؤولٌ عن إدارة الحسابات التجارية لشركة الواجهة، ويراقب المناقلات

المالية العالمية بمختلف العملات، بما فيها شركات خدمات الدفع على الإنترنت التي لا تفرض أية قواعد "للتعرف إلى الزبون" مثل ليبرتي ريسيرف.

المدير المعلوماتي

يحافظ المدير المعلوماتي على عمل البنية التحتية الحاسوبية للشركة الإجرامية وفي عهدته المخدمات الحاسوبية غير القابلة للتعقب "مضادة للرصاص"، ويتعاقد مع شركات استضافة فاسدة تقدم خدمات الإنترنت لضمان بقاء برمجياته الإجرامية بعيداً من متناول السلطات التنفيذية العالمية. كما يدير المدير المعلوماتي قاعدة بيانات "الزبائن" وجيوشاً من الروبوتات الشبكية، وهو المسؤول عن الأمن المعلوماتي الذي يشتمل أيضاً على إدارة "الشبكات الوكيلة" التي تحمي نشاطات عامليه وتضمن عدم تعقبهم. ويتولى المدير المعلوماتي أيضاً مهمة تشفير البيانات الإجرامية للشركة بما يضمن عدم تمكن السلطات أو منظمات القرصنة الإجرامية المنافسة من قراءة هذه البيانات أو استخدامها.

المدير التسويقي

كما تعلمت الكثير من الشركات القانونية، فإنّ مجرد توفر منتجٍ رائع لا يكفي في معظم الأحيان، فالأرباح تعتمد على قدرة الشركة (أو المؤسسة الإجرامية) على الترويج بفعاليةٍ لمنتجاتها وخدماتها. وبالطريقة ذاتها يعمل المدير التسويقي على تصميم إعلانات فعالة يقدمها إلى شبكات الاستضافة الإجرامية لتوزيعها في الأوساط السرّية الرقميّة.

الإدارة الوسطى

أي المديرين العملياتيين الذين غالباً ما يتم تجنيدهم عبر صداقاتٍ طويلة الأمد، وبعد أن يكون قد تم اختبارهم في الجريمة والدماء عبر فتراتٍ زمنية طويلة. هؤلاء هم المسؤولون عن إدارة معظم العمالة الإجرامية، إضافةً إلى

إدارة شبكات القيادة والتحكم التي تنفذ العمليات الإجرامية التقنيّة للمنظمة.

النحلات العاملة أو المُشاة

يشكل هؤلاء القوى الميدانية في معركة الجريمة، وهم يكافئون بائعي المخدرات الذين يقفون على ناصية الشارع. فهم يعملون بالتعاون مع عناصر أخرى من الشركة الإجرامية للمساعدة على توزيع البرمجيات الخبيثة عبر الروابط المصابة وملفات الـ بي.دي.إف ومواقع الويب المخترقة، وهم أيضاً يقومون بكسر رموز الكابتشا (تلك الكلمات ذات الحروف المتعرجة التي يجب على الناس كتابتها في مربع إدخالٍ نصي لإثبات أنهم بشر)، ويساعدون في توزيع أجهزة جمع معلومات البطاقات الائتمانية على متاجر التجزئة ومنافذ الصرافات الآليّة.

أقسام البحث والتطوير

كما في معظم المؤسسات، لا بد من وجود أقسام بحث وتطوير متقدمة للمحافظة على الموقع التنافسي، وليست العصابات الإجرامية استثناءً في ذلك. إذ يدأب قسم البحث والتطوير على التحري عن آخر الثغرات في البرمجيات المكتبية والتطبيقات النقالة والنظم الشبكية، وهي كلها فرصٌ يمكن تحويلها إلى مال في الأقسام الأخرى للشركة الإجرامية. إضافةً إلى ذلك، يمكن لفرق البحث والتطوير تولي مهام البرمجة المخصصة ذات الصعوبة غير الاعتيادية التي يتطلبها تعقبّ أهداف أو نظم بعينها.

المبرمجون والمهندسون والمطورون

يمثل هؤلاء الأدمغة التقنية ضمن الطاقم الإجرامي ويعتبرون مكوناتٍ أساسية في أية مؤسسة إجرامية شبكية. تقع على عاتق هؤلاء التقنيين مهمة تطوير الشيفرات الحاسوبية والبرمجيات التي تُعدي الأنظمة الأخرى، وهم

يقومون ببناء مواقع الويب وكتابة معظم البرمجيات الإجرامية وبرمجيات الفدية وبرمجيات الرعب، بما فيها برامج مكافحة الفيروسات المزوّرة التي يتمّ توزيعها من قبل مشغلي الشبكة الإجرامية. وهؤلاء هم من يقوم بكتابة البرمجيات الخبيثة الهجومية التي تصيب أنظمة المعلومات في العالم وتهاجمها. وبالطبع فإنّ الشيفرات البرمجية التي يكتبونها لا بدّ أن تخضع لإجراءات ضمان الجودة قبل أن يتم إطلاقها.

ضمان الجودة

يمثل فريق ضمان الجودة مفتاح النجاح في الشركة الإجرامية. فهو يضمن قدرة محارات التشفير التي يخبئ فيها المبرمجون برمجياتهم الخبيثة على تجاوز النظم الأمنية الحالية، كبرمجيات مكافحة الفيروسات وجدران النار. ويقوم مبرمجو ضمان الجودة باختبار جميع البرمجيات الخبيثة ومقارنتها بتعاريف مضادات الفيروسات المعروفة لضمان قدرة البرمجية الخبيثة على التخفي قبل إصدارها. وثمة أدواتٌ مثل avcheck.ru وScan4You.net تسمح لهذه الفرق بتقييم إمكانية اكتشاف هذه البرمجيات، بواسطة 18 من برامج مكافحة الفيروسات الأكثر شعبية. والأهم من ذلك هو أنّ نماذج تقدير إمكانية الاكتشاف هذه يتم تحديثها يومياً وهي مؤتمتةٌ بالكامل. بل إن مختبري ضمان الجودة الإجراميين يسجلون أنفسهم في قوائم الإشعارات، ليتم إعلامهم حين يتم اكتشاف البرمجيات الخبيثة التي يكتبها مبرمجوهم من قبل الشركات الأمنية وتصنيفها كبرمجياتٍ خطرة، إذ تسمح هذه الإشعارات للمبرمجين بتحديث برمجياتهم الخبيثة وتعديلها بسرعة بحيث يتعذر اكتشافها مجدداً ليستمر سير الأعمال.

المستضيفون

يتمتع التسويق بالاستضافة بشعبيةٍ هائلة ويحقق أرباحاً كبيرة في عالم

الإنترنت. وعادةً ما تحسب تكلفة التسويق بالاستضافة، الذي تتبعه أمازون وغيرها، وفقاً لعدد الزبائن الذي يجلبه إلى تاجر تجزئةٍ معين. وتشكّل شبكات الاستضافة العمود الفقري لشركة الجريمة السايبرية ويتموضع أفضلها في روسيا. وتعمل هذه المجموعات التي تسمى بارتنركاس ليلاً ونهاراً لتوجيه أكبر قدرٍ ممكن من الزائرين إلى مواقع شركائهم الإجراميين على الإنترنت. ويتولى مجرمو المستوى المتدني هؤلاء التوزيع الإعلاني للمنتج، سواءٌ كان برمجية مكافحة فيروسات مزورة أو مواد إباحية للأطفال أو ساعات روليكس مقلّدة أو فياغرا مزوّرة. وتتمثل مهمة المضيف في تقديم التاجر المجرم إلى الزبون الغافل. ويقوم أفراد البارتنركاس بنشر نماذجهم عبر البريد الإلكتروني المزعج، وفي المنتديات وعبر التعليقات في المدونات وفي الوسائط الاجتماعية وعبر الرسائل القصيرة. وتدفع الشركات الإجرامية لهؤلاء المستضيفين لقاء كل نقرة أو كل عملية تنصيبٍ تنتج عن توجيه المستضيف للزائرين إلى موقع المنظمة الإجرامية، أو لقاء كل مرةٍ يتم فيها تحميل البرمجية الخبيثة إلى آلةٍ ضحيّة. ويمكن للمستضيفين الإجراميين النشيطين أن يحققوا بسهولة دخلاً يصل إلى خمسة آلاف دولار في اليوم، علماً أن بعضهم يحقق 300 ألف دولار في الشهر. وكان من الشائع تاريخياً أن يوجه زعماء الجريمة المستضفين من مواقع الويب السريّة بأنّ "استخدام البريد الإلكتروني وغيرها من الطرق غير الشرعية التي تعتمد إصابة الآلة ممنوعةٌ منعاً باتاً". أجل لقد صار للشركة الإجرامية أيضاً شروط خدمة واتفاقيات ترخيص للمستخدم النهائي، تحمي من خلالها نفسها وتدحض أي ادعاءاتٍ بحقّ عامليها تتهمهم بأي ذنوبٍ إجرامية.

الدعم الفني

قد يكون شنّ حملات البرمجيات الإجرامية صعباً أحياناً. فتماماً كما نضطر أحياناً إلى إعادة تشغيل حواسبنا باستمرار أو إلى طلب المساعدة من قسم

تقانة المعلومات في الشركة أو إلى البحث عن حل على موقع بيست باي، كذلك هي حال المجرمين. لذا فإنّ عصابات الجريمة السايبرية الحديثة توفر الدعم الفني لكلٍ من موظفيها وشركائها.

مدير الموارد البشرية

يتطلب شنّ حملة جريمة عالمية بقيمة مئات الملايين من الدولارات، مثل إنّوفيتف ماركتنغ، بنجاح تضافر جهود الكثير من الأشخاص. ويساعد فريق الموارد البشرية على تجنيد الجنود الميدانيين أو النحلات العاملات الضروريات لتنفيذ العمليات اليومية في المشروع الإجرامي، حيث يقوم الفريق بإعداد بوابات ويب لمعالجة "إدارة رأس المال البشري"، التي تشتمل على طلبات العمل والرواتب والمستحقات، والتدريب على الشبكة الذي لا بدّ منه لتنفيذ حملة عدوى ناجحة بالبرمجيات الخبيثة. ويقوم مدير الموارد البشرية بوضع الإعلانات في الأوساط السرية الرقميّة، لتوظيف الشركاء الذين يعلمون تماماً أنّهم يعملون كجزءٍ من مؤسسة إجرامية. كما يساعد قسم الموارد البشرية على توظيف نوعٍ آخر من الموظفين يُدعون بالبغال، قد يعلمون أو لا يعلمون بأنهم يعملون مع مؤسسة إجرامية، وتقوم الإعلانات الموجهة للبغال على تقديم وعود بإمكانية تحقيق دخل عالٍ وبساعات عمل مرنة والقدرة على العمل من المنزل، وهي غالباً ما توضع على موقع لائحة كريغ أو حتى على مواقع التوظيف الشرعيّة على الويب. ويقوم كادر الموارد البشرية الإجرامي باستقبال المكالمات الهاتفية القادمة من المتقدمين للعمل، ويسارعون إلى الرد على جميع الأسئلة المتعلقة بميزات فرصة العمل وخطط الـ 401 كي الضريبية (التي يوعد المتقدمون بها إذا ما نجحوا في العمل لمدة عامٍ واحد).

بغال المال

يكمن مفتاح نمو أي منظمةٍ غير شرعيّة في نجاحها في غسيل الإيرادات الإجرامية. فلا بد من تحويل جميع الأموال المجنية، سواءٌ عبر تهريب المخدرات أو البرمجيات الإرهابيّة أو انتحال الهويّة، إلى أصولٍ شرعية ظاهرية بشكلٍ مناسب. ولتحقيق هذا الهدف يتم تجنيد "بغال المال" عبر شركات واجهة ليساعدوا على نقل المال مع إغفال الهوية من حسابٍ أو مصرفٍ أو بلدٍ إلى آخر. ويستجيب البغال على نحوٍ ساذج إلى إعلانات التوظيف، التي تحمل ألقاباً مثل مساعد محلي أو ممثل للشركة أو محاسب تسلُّم. ويتمّ إخبارهم بأنهم مسؤولون عن "معالجة عمليات الدفع" ويطلب إليهم فتح حسابين بأسمائهم، واحدٌ لتلقي الراتب وآخر لتحويل المبالغ التي يعالجونها، والتي عادةً ما تأتي عبر شركة ويسترن يونيون. وعلى البغال، الذين يتلقون على وجه العموم بين 3 و10 بالمئة من المبالغ التي يعالجونها، تقديم صورة عن هوية حكومية، الأمر الذي يعد مطلباً مهنياً منطقياً تماماً، لكنه يسهل على الشركة الإجرامية تتبع أية اختلاسات يتم اكتشافها في وقتٍ لاحق.

يشكل البغال وجه الجريمة السايبرية، وهم يعملون بأسمائهم الحقيقية، ما يعني أن صلاحيتهم لن تكون طويلة. إذ لن يمرّ وقتٌ طويل حتى تتصل الشرطة، وعندها فقط يعلم هؤلاء، ومعظمهم من ربات المنازل والطلاب والعاطلين من العمل لفترات طويلة، الذين كانوا قبل ذلك يغضون أبصارهم ويقتصدون في أسئلتهم بكل سرور، ليعلموا عندها أنهم متورطون في مشروعٍ إجرامي. وعندها تكون الأموال، و"الرؤساء" الذين كانوا يعملون بأسماءٍ مستعارة، قد ذهبت إلى غير رجعة. ووفقاً لأحد خبراء بغال المال، فإنّ النقص في حَمَلة المال هؤلاء يشكل عنق الزجاجة الأساسي الذي يواجه شركات الجريمة اليوم. فاختراق الأنظمة أمرٌ سهل، لكنّ تسييل الشكّات هو الجزء الأصعب. ويقدر الخبراء أن نسبة الحسابات المسروقة على البغال

المتوفرة قد تصل إلى عشرة آلاف مقابل واحد. بعبارةٍ أخرى لو توفرت الأعداد الكافية من البغال والموارد البشرية لكانت الخسائر المرتبطة بالجريمة السايبرية عشرة أضعاف ما هي عليه اليوم.

الشركة الناشئة (الإجرامية) المرنة

ليست بنية الشركة الإجرامية، مثلها في ذلك مثل أية منظمةٍ حديثة تتخذ من التقانة محوراً لعملها، ثابتةً في الزمان والمكان بل هي في حركة مستمرة. ففي كتابه "الشركة الناشئة المرنة: كيف يستخدم مقاولو اليوم الإبداع المستمر لخلق أعمالٍ في غاية النجاح"، يشرح إريك ريس طرقاً تسمح للمقاولين المبتدئين بخلق منتجاتٍ جديدة "تحت شروطٍ من الشك الفائق". أما بالنسبة للمجرمين، فإن الشك هو الميدان الذي يبرعون فيه، فهم لا يعلمون متى تأتي مداهمة الشرطة التالية أو متى يحدث تبادل إطلاق النار المرة القادمة مع عصابةٍ منافسة. والخارجون على القانون لا ينفكون يتكيفون ويبتكرون لتجاوز العقبات التي تقف في طريقهم ولتلبية آخر متطلبات السوق. فهم يبنون ويقيسون ويتعلمون باستخدام أدوات تحليل الويب المعتمدة على البيانات ويحتفظون بمعايير جيدة حول منتجاتهم وحول شركائهم. لكن ليست جميع المشاريع الإجرامية على الإنترنت موجهةً نزولاً من الإدارة حتى النحلات العاملات، فبعضها أكثر مرونةً وديناميةً بكثير.

تنسجم المنظمات الإجرامية أكثر مع غيرها مع العالم الذي يقدّمه توم فيريس في مفهومه لأسبوع العمل المؤلف من أربع ساعات، ويعتمد على تبسيط الأعمال التجارية وإزالة الأعباء عنها وأتمتة الأنظمة. حيث يتم تجنب البنى التنظيمية الثقيلة والقيادة المباشرة لأنها لا تتفق مع المنتجات والخدمات الفورية التي غالباً ما تكون قادرةً على تجميع نفسها عند الطلب. فالعاملون السرّيون على الشبكة ربما يكونون أكثر ميلاً للاهتمام

بالموازنة بين الحياة والعمل، أو لتصميم نمط الحياة بما يسمح لهم بالموازنة بين الجريمة واللهو، مع أعظمة الفرص المتاحة لهم على الجانبين. فهم يأتون معاً في أسرابٍ تمثل مجموعاتٍ من الأفراد في حركةٍ ثابتة. ويساهمون من خلال مهاراتٍ محددة لتحقيق هدفٍ مشترك، أما منتجهم فيكون عابراً وغير واضح المعالم في آن معاً، ما يجعل فرض القانون في غاية الصعوبة. وما إن يتم تنفيذ المهمة الإجرامية، مثل السطو على سمسار بيانات كبير أو بائع تجزئة، حتى تتفرق المجموعة إلى أن تجتمع مع آخرين لإنجاز المهمة الإجرامية التالية.

يشكل عناصر مثل هذه الأسراب الإجرامية الشبكيّة أحياناً محاور مختلفة بناءً على التخصص الإجرامي، فقد تقوم عصابة انتحال هويّة على سبيل المثال عفواً بتشكيل محورٍ معين، باستخدام مجموعاتٍ مختلفة من المهارات تستحضرها من عدة أسراب، فتتولى مجموعةٌ من المشاركين تتمتع بمهاراتٍ تقنيةٍ عالية مسؤولية اختراق نظم بياناتٍ تجاري، بينما تؤدي المجموعة التالية دور سمسار البيانات بأن توزّع المعلومات الشخصية المسروقة إلى خبراء تزوير الوثائق، الذين يُعدّون شهادات قيادة وبطاقاتٍ ائتمانيّة وشيكات وجوازات سفر باستخدام هذه المعلومات. وتقوم أسراب العصابات المتدنية المستوى، التي تقوم بتنفيذ عمليات الاحتيال المالي الفعلية، بتحويل أية مبالغ تتلقاها إلى شبكة البغال التي تقوم بدورها بالتعاون مع شبكات غسيل الأموال لضمان تسديد الأموال إلى جميع الأطراف الإجرامية، لقاء الخدمات التي قدمتها وتلقي نصيبها من الإيرادات الإجرامية. في عالمٍ تسوده شركات الجريمة وشبكات الأسراب الإجرامية يكون الأمن العملياتي في غاية الأهمية، حيث يتم تنفيذ العمل وإجراء الاتصالات عن بعد لتجنب الحاجة إلى اللقاءات الشخصيّة، ويتم تقسيم العمل وتوزيعه على طبقات لضمان عدم معرفة المشاركين في المستويات المتدنية

بالهويات الحقيقية للأطراف الأخرى المشاركة في الجريمة. وتوفر منتديات القرصنة على الإنترنت وقنوات الاتصال فيها نقاط تعارف وتجنيد وتجمّعاً للمتآمرين الإجراميين، تمكنهم من التنسيق بين أطراف السرب الذي لا بد منه لإتمام العمل في مشاريع محددة.

مصفوفة الجريمة المعقدة

بصفتي المدعى العام في مانهاتن، قليلةٌ هي الأشياء التي تقلقني كما يقلقني التهديد السايبري الذي يرصّ صفوفه اليوم.
بريت بارارا، المدعي العام لمديرية جنوب نيويورك

سواءٌ اتبعت مجموعات الجريمة السايبرية المنظمة الأشكال التنظيمية السائدة في الشركات، كما فعلت شركة إنّوفيتف ماركتنغ، أو اتخذت شكل الأسراب الرشيقة التي تجمع نفسها بنفسها، فإنّ شيئاً واحداً يبقى واضحاً: إنها تتبع أسلوباً معقداً في إجراء أعمالها ومتابعة "زبائنها". فهي تتبنى أحدث الاستراتيجيات التجارية التي تتبعها المنظمات الشرعيّة. وهي ضليعة في مجال إدارة السلاسل واللوجستيات الشاملة والمالية الإبداعيّة والتصنيع الفوري وتحفيز العاملين وتحليل حاجات الزبائن. والنتيجة هي مؤسسة الجريمة السايبرية الحديثة، وهي منظمةٌ كاملة الخدمات متعددة المنتجات عالية الربحيّة، عالميّة قادرة على النيل من أي فردٍ أو شركة أو حكومة إذا ما رغبت في ذلك. وكما نوهنا سابقاً، ثمة ما لا يقل عن خمسين منظمة إجرامية على الشبكة من هذا القبيل تعمل حالياً في أنحاء العالم.

لقد خبرت بنفسي مدى هذا التعقيد، حين كنت أعمل مع الإنتربول والشرطة الفيدرالية البرازيلية على قضايا تشتمل على بطاقات ائتمانية مسروقة في أنحاء أميركا اللاتينية. ففي العشوائيات التي تحيط بمدينة ريو دي جانيرو كانت عصابات الجريمة السايبرية المنظمة تبيع برامج على أقراص دي.في.دي تحتوي عشرات الآلاف من أرقام البطاقات الائتمانية

المسروقة وتفاصيل مستخدميها، وكانت الشركات الإجرامية الناشئة تبيع هذه الأقراص إلى المجرمين الآخرين مقدمةً تنزيلاتٍ على المشتريات بالجملة. بل إنها كانت تشمل برمجياتها باتفاقات مستوى الخدمة، مؤكدةً أن 80 بالمئة من أرقام البطاقات الائتمانية المسروقة التي نقدمها على الأقل سيعمل وإلا "استعد نقودك". بل إن البرازيليين قدموا أرقام هواتف للدعم الفني يمكن للمجرمين الآخرين الاتصال بها حين يواجهون صعوبات تقنيّة بينما يحاولون تعلم استخدام هذه البرمجيات. "هل جربت يا سيدي إعادة تشغيل الحاسب؟".

تستخدم بعض منظمات الجريمة بالفعل برمجيات إدارة العلاقات مع الزبائن، لتتبع طلبات الزبائن وبناء الولاء لعلامتها بين زبائنها الإجراميين كما فعل أصحاب الشركة الناشئة، التي طورت حصان طروادة المعروف باسم سيتادل. وكانت هذه البرمجية الخبيثة، وهي نسخة معدلّة من حصان طروادة المعروف باسم زيوس، تسمح للمجرمين بسرقة المعلومات البنكية وتسجيل نقرات المفاتيح للمستخدمين وتنصيب أشكال أخرى من البرمجيات الإجرامية على آلة الضحيّة. وحين كان قراصنة سيتادل يبيعون برمجياتهم الخبيثة إلى زملائهم المجرمين، كانوا يرغبون بضمان رضى زبائنهم عن البرمجيات الإجرامية التي طوروها. ومقتبسةً بصفحات من مواقع مارشال فيلد وهاري كوردن سيلفردج، تعهّدت عصابة سيتادل بأنّ "منتجاتنا سيتم تحسينها وفقاً لرغبات زبائننا" وكانت تعني ما تقول. فقد أنشأ مطوروها واجهة مستخدم لإدارة العلاقات مع الزبائن، تسمح لزملائهم المجرمين الذين يستخدمون برمجيات سيتادل الخبيثة المتخصصة بسرقة المعلومات المصرفيّة بالإبلاغ عن الأخطاء، وباقتراح الميزات الجديدة وبالتصويت عليها ليتم شملها في النسخ القادمة من البرمجية، بل حتى بإنشاء تذاكر مهام للمطورين. وكان توفير الدعم الفني يتم عبر المحادثة

المباشرة على أي.سي.كيو وجَبَر وكانت معالجة تذاكر المشكلات تجري بدأبٍ، بل إن المنظمين الإجراميين لسيتادل قاموا بإنشاء شبكةٍ اجتماعية تسمح لـ "الأشخاص ذوي العقليات المتشابهة" الذين يستخدمون حصان طروادة المصرفي بالاجتماع ومناقشة "مشاريع تحظى باهتمامٍ متبادل" مثل سلبنا أنا وأنت.

يمكن لشركة الجريمة أن تكون عقلانية ومنطقية إلى حدٍ بعيد، حيث تستخدم تكتيكاتٍ مشهوداً لها للحفاظ على تفوقها التنافسي وضمان استمرار عملياتها، الأمر الذي يعني في الأوساط السريّة الرقميّة تتبع تطور المنافسين وترقب الاضطرابات التجارية المحتملة، خصوصاً تلك التي تتسبب بها السلطات التنفيذية. وكما رأينا سابقاً، فإنّ القراصنة المجرمين لا يكتفون بمراقبة نشاطات وكالات الشرطة ذات الصلة ومسؤوليها، بل إنهم يجمعون أيضاً معلومات استخبارية مفتوحة المصدر للكشف عن أية تهديدات قد تطال أرباحهم الهائلة. فقد قامت إحدى مجموعات اللصوص السايبريين، والتي كانت مسؤولةً عن اختراق جيت بلو وسيفين ايلفن وجي.سي.بيني وسوق ناسداك للأوراق المالية، بإنشاء نظام "أسلاك تعثُّر" توفر نظام إنذار مبكراً ينبهها في حال عُلم بالاختراقات التي تقوم بها وانتشرت الأخبار. لمزيدٍ من الدقة، قامت المجموعة بإنشاء مجموعة من تنبيهات غوغل مع اختيار الكلمات المفتاحية بعناية بحيث تغطي ضحاياها المستهدفين، فحالما تُنشر قصصٌ إخباريّة حول "اختراق ناسداك"، يمكنها سحب أسهمها والخروج قبل أن تتّبعها الشرطة. لقد أصبح القراصنة يمثلون المافيا الجديدة وهم يساهمون يومياً في العملية المستمرة في التحويل الصناعي للجريمة وزيادة احترافيتها.

الشرف عند اللصوص: الشيفرة الإجرامية للأخلاق

إذا أردت أن تكون ناجحاً في عالم الجريمة فلا بد لك من سمعة النزاهة.

تيري براتشت، قَدَم من صلصال

للمحافظة على تنظيم وعمل اقتصاد الجريمة السري K لا بدّ لشركات الجريمة من مراقبة بعض قواعد السير. والحال، فإنّه ثمة بالفعل شرفٌ بين اللصوص، بل إن بعض عناصر شركات الجريمة تقوم بنشر "قواعد السلوك" لتساعد على طمأنة الزبائن الإجراميين الزملاء. فهذه الأسواق السايبرية السوداء حسنةُ التنظيم وذاتية الرقابة يقوم فيها الشراةُ والباعة باستمرار بتقييم سمعة أحدهم الآخر والمصادقة عليها. بل إنّ بعض الأسواق الإجرامية الرقميّة تُقدم نظم نجوم السمعة التي تسمح للقراصنة الزملاء بتقييم البطاقات الائتمانيّة المسروقة وشهادات القيادة المزوّرة والفيروسات الحاسوبية بمنحها عدداً من النجوم يتراوح بين الصفر والخمسة، تماماً كما يحدث على إيباي أو آي.تونز.

وفي أسفل قاعدة السوق الإجرامية الشبكية، هذه المستويات التي يسهل الوصول إليها، لا تكون خروقات القواعد السلوكيّة نادرة. فهؤلاء الأفراد معروفون بأنهم "مارقون" يفشلون في تقديم البضائع أو الخدمات الإجرامية الموعودة في ما يصل إلى 30 بالمئة من الحالات. لكنهم ما إن ينكشف أمرهم حتى يتم الإبلاغ عنهم بسرعة ومنعهم وطردهم من السوق، تماماً كأي بائع على موقع إيباي أو أمازون يفشل في ايصال ما وعد به. وللتغلب على مشكلات الثقة هذه، قام المجرمون السايبريون بالفعل بتأسيس بيوت فوترة وخدمات تعاقد تماماً كتلك التي ستستخدمها حين تشتري أو تبيع منزلاً. ويساعد هؤلاء السماسرة النزيهون، لكن الإجراميون، على ضمان التسليم الفعلي للمنتج غير القانوني أو للبيانات المسروقة، فعندها فقط يسملون المبالغ التي في عهدتهم بعد أخذ خمسة بالمئة عمولة صفقة لقاء خدماتهم.

أما على المستويات العليا في الشركة الإجرامية، فإن الداخلين الجدد إلى

الأوساط السرّية السايبرية يخضعون لتمحيصٍ دقيق، ولا بد لهم من كفالة طرفٍ موثوق، تماماً كتجار المخدرات الذين لا بد لهم من تسلق السلم درجةً درجة. هنا، حيث يلعب الأطفال الكبار، تكون اختراقات قواعد السلوك نادرةً وتبعاتها عالية. فجميع الأطراف تعلم أنه من مصلحتها اتباع القواعد، وتماماً كما ينتشر الانتقام في أوساط الجريمة المنظمة التقليدية فإنه ينتشر أيضاً في الأوساط السرية السايبرية. وإذا كان تبريح المنافسين ضرباً ورميهم في نهر ايستريفر بأحذيةٍ من الإسمنت هو علامةٌ فارقة لرجال عصابات المدرسة القديمة، فإن لدى الأنداد الرقميين لهؤلاء أساليبهم غير اللطيفة أيضاً. ومعارك السيارات تحدث أيضاً، كالهجوم السهمي الذي استمر ليومين وشنّه ماكسري فيجن (المعروف أيضاً بآيسمان)، حين درّب أسلحة لوحة مفاتيحه على طبيعة منافسيه ليفنيهم. فمن شقته في سان فرانسيسكو، تمكن آيسمان من السيطرة على قواعد بيانات المعلومات الخاصة بمنافسية الإجراميين وسحبِ محتوياتها واستخدامها لإنشاء موقعه الكبير الخاص كاردرس ماركت، الذي نما ووصل عدد أعضائه إلى ستة آلاف عضو. وباستخدام البيانات المسروقة من منافسيه، استطاع الموقع جمع أكثر من مليوني بطاقة ائتمانيّة مسروقة، منتزعاً 86 مليون دولار في مناقلات احتياليّة. تؤدي المهارات التقانية المميزة دوراً مهماً في عالم شركات الجريمة، والقراصنة لا ينفكون يدرسون ويتعلمون لتحسين قدراتهم.

الجريمة يو

ما من أحدٍ يولد قرصاناً، فالقراصنة يتم تدريبهم ودعمهم ومنحهم فرص التعليم الذاتي عبر مقادير هائلة من المواد التعليمية المجانية المتوفرة في الأوساط السريّة الرقمية. فشركة الجريمة هي منظمةٌ تعليمية، وثمة دروسٌ على الإنترنت لتعليم أي شيء، من كسر الجدران النارية إلى استنساخ البطاقات الائتمانيّة. تتوفر للمجرمين دورات جماهيرية مفتوحة على

الشبكة خاصة بهم، يمكنهم من خلالها تعلم شنّ حملات التصّيد وحملات البريد المزعج، إضافةً إلى استخدام البرمجيات الإجرامية وأدواتها الهجومية. ويرقى كل هذا التدريب إلى نوعٍ من الجامعة الإجرامية الشبكيّة (جامعة الجريمة)، ساهمت في تقدم مهارات القراصنة الإجراميين الأفراد. ومن المثير أن نرى مشرفين يكونون في الحقيقة من القراصنة الزملاء يجتمعون كثيراً مع بعضهم لمساعد المستجدين على تعلم صنعة الجريمة الرقميّة. وثمة الكثير من صفحات الويكي التي يتم إعدادها في أماكن كثيرة في العالم السري السايبري تقدم روابط تشعبيّة تفصيلية مرتبة حسب الفئة، تشرح كيفية اختراق أي جهازٍ أو تطبيقٍ أو برمجية أو نظام تشغيل موجود على الإطلاق.

لا تتم جميع التدريبات الحاسوبية الجانحة والمحظورة في العالم الحر بالطبع. فالسجون، التي غالباً ما ينظر إليها كـ "مدارس ختامية" للمجرمين، لا تساهم سوى بقدرٍ ضئيل في إعادة التأهيل، بينما تساهم كثيراً في تخريج طلاب الجريمة. بل إنّ دراسةً أجرتها جامعة أويو، بيّنت أنّ "الأفراد ذوي السوابق يحققون دخلاً سنوياً أعلى بكثير عبر الإيرادات غير الشرعيّة، مقارنةً بأولئك الذين ليست لديهم سوابق، حيث يحققون وسطياً 11 ألف دولار إضافية من الدخل الإجرامي كل سنة". وتماماً كما تحسن الجامعة فرص الدخل لدى أولئك العاملين في الاقتصاد الشرعي، يمكن تحقيق الشيء نفسه عبر التخرج من مدارس ما خلف القضبان.

لذا فإنّه قد يكون من المفاجئ أن يقوم المزيد من السجون بتقديم تدريبٍ على الحاسوب والبرمجة لسجنائها. فبقدر ما يمكن لهذه المهارات أن تكون المفتاح للبدء بمسيرةٍ مهنيّة قانونية بعد الخروج من السجن، يمكنها أيضاً أن تكون مفيدةً لأهدافٍ غير شرعيّة، حتى من داخل السجن. وهو ما حدث مع نيكولاس ويبر خلال فترة سجنه في سجن جلالتها في إيسس شمال لندن، حين استخدم مهاراته الحاسوبية الذي اكتسبها خلال تدريبٍ على

الحاسب لاختراق نظام الحاسب الخاص بالسجن. وفي سجن سان كوانتين الشديد الرقابة في الحديقة الخلفية لوادي السيليكون، أسسّ ضباط الإصلاح هناك حاضنةً للشركات الناشئة مخصصةً للسجناء ذوي الطموحات التجارية. وبدعمٍ من الهيئات التقانية المحلية، شارك السجناء في "أيام عرض" يستعرضون خلالها أفكارهم ليقوم مديرون تنفيذيون من وادي السيليكون بالحكم عليها وتقدير قدرتها على النجاح. ومع أنّ القصد من وراء هذه البرامج جديرٌ بالثناء، فإن نتائجها من الناحية العملية قد تختلف إلى حدٍ كبير عن النتائج المتوقعة.

الإبداع القادم من العالم السفلي

من المكونات الأساسية للإبداع القدرة على تحدي السلطة واختراق القواعد.

فيفيك وادوا

لطالما كان المجرمون، المجبرون على العمل خارج النظم الشرعيّة للسلطة، خبراء في التفكير الحر وفي ابتكار حلول جديدة للمشكلات الصعبة. فهم يُبدون مرةً تلو الأخرى قدرةً هائلة على الاختراع في ممارساتهم المهنيّة وعلى الاستخدام المبتكر للموارد. وهو ما يلخصه جي.كي.تشسترتون في قصته القصيرة "الصليب الأزرق"، حين يعلن بدماثة أنّ "المجرم هو الفنان المبدع، أما المحقق فما هو سوى الناقد". أما الجانب المظلم من هذا الإبداع فيمكن مشاهدته يومياً في عالم شركة الجريمة. ويكمن التحدي التي تقف أمامه بقية المجتمع في أن الابتكار التقاني مستمرٌ بوتيرةٍ أسّية وفي أنّ قانون مور، وهو الأهم، ينطبق على المجرمين أيضاً.

إنّ الإبداع التقاني في العالم السفلي يزدهر، وعقلية القفير الإجرامي تتجاوز قدرات شركات مكافحة الفيروسات وبائعي التقانة والسلطة التنفيذية. إذ لم تعد القرصنة ميداناً لقلةٍ من المعلمين الرقميين، بل

أصبحت اليوم ديمقراطيةً تتيح جميع المعلومات الضرورية عبر جامعة الجريمة. والمجرمون الحديثون يبتكرون، لا فقط تقانياً، بل أيضاً في نماذجهم التجارية. إذ تتبنى شركة الجريمة اليوم نماذج اشتراك لخدمات البرمجيات الخبيثة، وتطبق استراتيجيات التلعيب لمهام كوادرها وتستخدم مناهج تطوير البرمجيات مفتوحة المصدر لتكديس أحصنة طروادة. وللدفع بمبيعاتها، تعرض الشركة الإجرامية على المحتالين الزملاء نسخاً مبسطّة من الأدوات البرمجية غير الشرعيّة، بل إنها قد تقدّمها مجاناً. فإذا كان زبائنها الأشرار سعداء بالمنتج، يمكنهم دفع المزيد لقاء ترقية البرمجيات والحصول على النسخ الكاملة، وهي استراتيجيةٌ معروفة باسم تسعير الفريميوم.

يتّبع المجرمون السايبريون المنظمون إلى حد بعيد استراتيجية كريس أندرسون المعروفة باسم "الذيل الطويل"، ويرون مستقبل الأعمال الإجرامية في سرقة القليل مقابل المزيد. فبينما كان مجرمو الأمس يسعون طوال الوقت خلف غارة العمر الوحيدة (كما في فيلم أوشينز ايليفن أو كما في ماسة النمر الوردي)، تعلم سفاحو اليوم السايبريون أن بإمكانهم تحقيق أرباح هائلة ببساطة عبر تنفيذ عملياتٍ أصغر مراراً وتكراراً مستهدفين بها الجماهير. وكما سنرى في الفصل القادم، فإنّ الكثير من عمليات السرقة الصغيرة هذه يمكن أتمتتها بما يؤدي إلى دفقٍ مستمر من الدخل المتكرر مع خطر اعتقال أقل.

لتحفيز قاعدة عمال إجراميين متنوعة توصل مسؤولو شركة الجريمة إلى عددٍ من نماذج التشجيع للحفاظ على زخم أعمالهم. فبالنسبة لكثيرٍ من القراصنة، لا يشكل المال الدافع الوحيدة، فكثيرٌ منهم تفتنه فكرة خرق القانون أو التحدي الكامن في اختراق نظامٍ أمني معقد أو التفاخر بالحقوق التي يحصل عليها من جراء الاحتيال على مثل هذا النظام. وقد أسّس أعضاء الأوساط السريّة السايبرية مواقع ويب تسمح للقراصنة الزملاء

بمراجعة الهجومات الرقميّة التي يقوم بها زملاؤهم وتقييمها. فموقع RankM يمنح نقاطاً لأفضل الأفضل ويستخدم هيئاتٍ قيادية لفصل الراغبين بالانضمام عن نخبة القراصنة.

يدرك زعماء الجريمة السايبرية جيداً هذه النزعات، وقد توصلوا إلى طرقٍ متنوعة لتلبية احتياجات الموظفين إلى الاعتراف والتحدي والانتماء، عبر تضمين عناصر من التلعيب في نشاطاتهم الإجرامية. ففي مونتينغرو، أقامت عصابة كليك.في.آي.بي للبرمجيات الإرهابية حفلةً لمنصبي البرمجيات الخبيثة الأكثر إنتاجية، عرضت فيها محفظةً كبيرة مليئةً بأوراق اليورو للشريك الذي أصاب أكبر عددٍ من الآلات. وفي بداية عام 2014، وسعياً لدفع الإبداع وخلق خطوطٍ جديدة لهذه الأعمال الشائنة، عرض مسؤولٌ أوروبي شرقي في شركة إجرامية سيارة فيراري جديدة للقرصان الذي يخترع أفضل طريقةٍ للاحتيال. وتم الكشف عن أخبار الجائزة في زاويةٍ مظلمة من العالم السرّي الرقمي، عبر فيديو احترافي الإخراج تظهر فيه العديد من "المساعِدات" الفاتنات على أرض صالة العرض الخاصة بالتاجر. وسرعان ما أتت استراتيجية التلعيب ثمارها ونالت اهتماماً واسعاً بين العاملين، بينما تم حجز الفيراري لـ "عامل الشهر" المختار.

من التعهيد الجماهيري إلى تعهيد الجريمة

من بين جميع تقنيات الإبداع التجاري التي تتبعها الشركة الإجرامية، ما من تقنيةٍ أكثر انتشاراً من التعهيد الجماهيري. بدأ التعهيد الجماهيري كأداةٍ شرعيّة للاستفادة من حكمة الجماهير لحلّ مشكلاتٍ معقدة تجارية وعلمية. وقد طُرح مفهوم التعهيد الجماهيري لأول مرة وحظي باهتمامٍ واسع في مقالةٍ كتبها عام 2006 جيف هاو لمجلة وَيَرد، حيث عرف هاو التعهيد الجماهيري بأنّه عملية "التعهيد الخارجي لمهمة إلى مجموعةٍ من الأشخاص كبيرة وغير معروفة عبر نداءٍ مفتوح". وإذا كان ثمة مئات الأمثلة

لعمليات التعهيد الجماهيري التي تم توثيقها مع نتائج باهرة، فإن هذه التقانات نفسها يمكن استغلالها لأهدافٍ إجرامية أيضاً.

يعج موقع يوتيوب بأمثلةٍ كثيرة لأشخاصٍ يبدون غرباء يبدأون فجأةً بالغناء، سواءٌ في مطار هيثرو أو في ساحة التايمز. لكن ومضات الغوغاء هذه قد تتحول بسرعةٍ إلى "ومضات سطو" يجتمع فيها غرباء أقل حسن نيّة ليس بهدف الفن بل بغرض الجريمة. وعلى الرغم من أن ومضات السطو هي من أدوات العصابات المتدنية المستوى في أغلب الأحيان، فإنها تحقق نجاحاً كبيراً. ففي واشنطن العاصمة قام ثلاثون من الشبان، كانوا جميعاً ينسّقون على الوسائط الاجتماعية وبواسطة الرسائل القصيرة، في وقتٍ واحد باقتحام متجر جي - ستار رو وهربوا بملابس تصل قيمتها إلى عشرين ألف دولار، متغلبين بسهولة على مشرفي المتجر. ولو ألقي القبض على أي من المشاركين في العملية لكان من غير الوارد أن يتمكن من الوشي بزملائه المتآمرين الذين قابلهم للمرة الأولى في مسرح الجريمة. وثمة حوادث مشابهة قد سُجلت في شيكاغو وفيلادلفيا ولوس أنجلوس.

ثمة تقنيات تعهيد جماهيري تهدف إلى مساعدة أولئك الذين قد يخترقون القانون على تفادي الشرطة. ففي الولايات المتحدة ثمة تطبيقاتٌ نقالّة، مثل دوي دودجر وبَزّيد وتشيكبوينت وينغمان، تسمح لأولئك الذين أسرفوا في الشراب باستخدام التعهيد الجماهيري لتحديد مواقع نقاط التفتيش التي تجري اختبار القيادة تحت تأثير العقاقير، واستعراض هذه النقاط على خريطةٍ تفاعلية على جهاز الآيفون أو الأندرويد، وتلقي إنذاراتٍ حين يتم تحريك نقاط التفتيش أو عند تنصيب نقاط جديدة. وحين تحولت أعمال الشغب في لندن عام 2011، التي بدأت اعتراضاً على خطط تقليص الإنفاق، إلى العنف، أنشأ المحتجون تطبيقاً يدعى ساكي يسمح لهم بتصوير الشرطة وتحميل صور مزودة بسمات جغرافية إلى الخريطة التفاعلية العاملة

بالتعهيد الجماهيري، فكان المشاركون في الاحتجاجات حين يشغلون التطبيق على أجهزتهم يعلمون بمناطق انتشار شرطة مكافحة الشغب، ويتلقون بُوصَلات تفاعلية تشيرُ عليهم بطريقة تجنب رجال الشرطة (بتمييز المناطق الآمنة بالأخضر ومناطق خطر الشرطة بالأحمر).

قام النشطاء القراصنة بدورهم بالاستفادة من تقنيات التعهيد الجماهيري جيداً، ففي ذروة نزاعه مع سوني ومجموعة نيوز كورب، لم يتورع لولزسِك عن تأسيس خط هاتفي ساخن يقدم معلومات عن الهدف التالي الذي يجب على الناشطين القراصنة استهدافهم. حيث قامت المجموعة بتخصيص رقمٍ هاتفي في أوهايو، وسجلت رسالة تحيّة مع لكنةٍ فرنسية تقول للمتصلين "لسنا متوفرين الآن لأننا مشغولون بنهب الإنترنت"، طالبة من المتصلين ترك طلبات القرصنة الخاصة بهم بعد الإشارة. وتسمح طريقة إدارة الأعمال الجديدة هذه بتعهيد الجريمة سامحةً للجماهير بالتصويت، على غرار أميركان آيدول، لتحديد ضحية الجريمة التالية. وقد أعلنت المجموعة في ما بعد في بيانٍ لها أنّها شنّت بنجاح هجمات حجب خدمة ضد ثمانية مواقع تمّ اقتراحها من قبل المتصلين. يمكن تعريف التعهيد الإجرامي بأنه أخذ العمل الإجرامي، كله أو جزء منه، وتعهيده إلى جمهورٍ من الأفراد العالِمين أو غير العالمين بالأمر.

عبر اعتمادها العنيف تقنيات التعهيد الجماهيري، باتت شركة الجريمة قادرةً على بناء شبكات توزيع إجرامية مغفلة الهوية واسعة، يمكنها تنظيم نفسها والتجمع بسرعةٍ مدهشة. ولتوضيح حجم هذه القدرات، نذكر هنا أن زعماء شركة الجريمة في روسيا وأوكرانيا، تمكنوا عام 2013 من إطلاق مئة من بغال المال على مشفى في ولاية واشنطن كانوا قد اخترقوه. وكانت النتيجة هي سرقة أكثر من مليون دولار من نظام محاسبة المشفى وغسيلها عبر 96 حساباً مستقلاً خلال بضعة أيامٍ فقط. وكما نوهنا سابقاً، فإنّ كثيراً

من هذه البغال ربما كان قد اختير دون معرفته من قبل الجريمة المنظمة، معتقدين "أنهم يعملون من المنزل" كـ "ممثلي تحصيل مستحقات محليين".

بفضل التقانة، أصبح بإمكان شركة الجريمة تعهيد عملها إلى شركاء غير مدركين للأمر على نحوٍ أسهل من أي وقت مضى، دون أن يدرك هؤلاء أنهم يشاركون في هجومٍ غير شرعي. إذ يحتاج المجرمون، على سبيل المثال، إلى دفق مستمر من حسابات البريد الإلكتروني الجديدة، يستطيعون من خلالها شنّ هجمات البريد المزعج ورسائل التصيّد، لكن نظام الكابتشا قد يبطئ عملهم. وللالتفاف على هذه المشكلة، طور المجرمون نظاماً برمجياً يأخذ آلياً صور الكابتشا التي يتم عرضها على ياهو أو هوتميل ويقدمها لأشخاص غرباء بشكلٍ عشوائي ليقوموا بحلّها. لكن ما الذي سيدفع شخصاً غريباً لفعل ذلك؟ الحل بسيط، فقد تمّ تحفيز هؤلاء على أحسن وجه عبر المحتويات الإباحية. فللاستفادة من التعهيد الجماهيري لحل مشكلتها، أنشأت شركة الجريمة العشرات من المواقع الإباحية المجانية التي تطلب من زوارها حل رمز الكابتشا لإثبات أنهم بالغون ولكي يتمكنوا من الوصول إلى المحتويات. إلا أنّ الأحاجي التي كان الجمهور المتعطش للجنس يعمل على حلّها لم تكن سوى رموز الكابتشا الفعليّة التي يحتاج إليها المجرمون لإنشاء حسابات البريد الإلكتروني معروضةً عليهم بعد قصها ولصقها بالزمن الحقيقي. وفي هذه الحالة تخرج جميع الأطراف رابحة، حيث يقدم المحتوى الإباحي العالي الجودة مقابل مشاركة الغافلين عبر التعهيد الجماهيري في هجوم تصيّد.

مع أنّ مفهوم الكاتبشا كان ذكياً، فإنه يصبح باهتاً إذا ما قورن بإعلان فرصة عملٍ إجرامية ينشر على الإنترنت. ففي سياتل في واشنطن قام لصُ بنوكٍ بدراسة برنامج شاحنةٍ مدرّعة، كان يفترض أن توصل مبلغاً كبيراً من

المال إلى فرعٍ محلي لمصرف أميركا. ففي ذلك الثلاثاء، وفي الساعة الحادية عشرة تحديداً قصد اللص، مرتدياً بزّة سلامة صفراء ونظارات وقميصاً أزرق وحزام أدوات وقبعةً مقوّاة وقناع تنفس، حارس السيارة المدرّعة الذي كان يحمل في يديه العديد من الحقائب الكبيرة المملوءة بالمال متوجهاً بها إلى البنك، ورشق وجهه برذاذ الفلفل، ففقد الحارس توازنه وأسقط حقائب المال على الأرض، ليتلقفها اللص ويدفعها إلى كيس خيشٍ كبير كان قد أحضره معه، قبل أن يهرب بما يحمل من "مبلغٍ محترمٍ جداً من المال" على حدّ تعبير المصرف. وحين استعاد الحارس وعيه، أطلق نداء استغاثة عبر اللاسلكي مقدماً أوصاف لص المصرف. وسرعان ما تجمعت عدة سيارات شرطة مطلقةً أضواءها وصفارات إنذارها في مسرح الجريمة بحثاً عن عامل البناء الذي هرب لتوه بغنيمته.

تمكنت أول سيارة شرطة تصل إلى المكان من مشاهدة عامل البناء بالفعل، فصوبّ رجال الشرطة بنادقهم إليهم، مطالبينه برفع يديه إلى أعلى والركوع على ركبتيه. ثم شاهدت سيارة شرطةٍ أخرى عامل البناء المتهم مرةً أخرى، ثم شُوهد عاملٌ آخر وآخر. كان في مسرح الجريمة في الحقيقة عشرات عمال البناء الذين تطابق مواصفاتهم الوصف الذي قدمه حارس السيارة المدرعة، فما لم تدركه السلطات هو أنّ اللص الفعلي كان قد استخدم التعهيد الجماهيري بدقة ليخطط انسحابه مسبقاً. فقبل عملية السطو بعدة أيام قام اللص الحقيقي بوضع إعلانٍ على قائمة كريغ في قسم البحث عن مساعدة، مدعياً فيه أنه يبحث عن عمال بناء لتشكيل فريق صيانة طرقات. وكانت التعويضات كبيرةً تصل إلى حوالى 30 دولاراً في الساعة، وطلب من الراغبين الظهور يوم الثلاثاء عند تمام الساعة الحادية عشرة عند التقاطع الذي يقع عنده مصرف أميركا. بل وطلب إليهم أيضاً أن يحضروا معهم أدواتهم الخاصة، بزّة سلامةٍ صفراء ونظارات وقميص عمل

أزرق وحزام أدوات وخوذةً وقناع تنفس. وبالفعل، فإن العشرات من الباحثين عن العمل ظهروا في المكان والزمان المحددين غير مدركين أنهم متورطون من دون علمهم في عملية سطوٍ على مصرف، تم تخطيطها عن طريق التعهيد الجماهيري. ففي عالم "الإيمان بالشاشة" يسهل خداع العامة. ولم تدرك الشرطة ما كان قد حدث إلا بعد أن جمعت جميع عمال البناء في المكان وحاصرتهم، لكن عندها كان اللص الحقيقي قد اختفى منذ وقتٍ طويل.

ليست شركة الجريمة سريعةً في تبني الأشكال الواعية وغير الواعية من التعهيد الإجرامي وحسب، بل هي أيضاً تستخدم نموذجاً شائعاً جداً في أوساط الشركات الناشئة هو التمويل الجماهيري. والتمويل الجماهيري أو الجماعي هو عمليةٌ يتم من خلالها جمع المال من جمهورٍ من الداعمين، يوافقون على دعم شركة ناشئة جديدة أو مشروعٍ غير ربحي، عادة ما يتم شرحه بالتفصيل على موقع ويب معين. والمواقع الأكثر شعبيةً في هذا المجال هي كيك ستارتر وإندي غوغو، وقد تم بالفعل تمويل عشرات الآلاف من هذه المشاريع بنجاح، حيث جمعت ما يصل إلى المليار دولار من الجمهور. والمجرمون سيكونون بالطبع سعداء باختراق أي شخصٍ يرفل في كل هذا المال، وقد سبق لهم أن اخترقوا موقع كيك ستارتر. وخطط التمويل الجماهيري لدى القراصنة الإجراميين هي أكبر بكثير وأكثر طموحاً، منها مثلاً اختراق جهاز الآيفون الذي في جيبك. فعندما أطلقت أبل هاتف الآيفون 5اس النقال، كان يشتمل على ميزة تاتش.آي.دي، وهي عبارة عن ماسح للبصمة تم تسويقه على أنه "طريقةٌ مريحة وفي غاية الأمان للولوج إلى هاتفك". وعلى الرغم من أن أبل ربما كانت قد أنفقت سنواتٍ وملايين من الدولارات على تطوير تقانتها البيومترية المحميّة ببراءة اختراع، فإنها بتقديمها هذه الميزة كانت في الواقع تضع تحدياً أمام القراصنة لقهر

"نظامها الذي يتمتع بأعلى درجات الأمن".

وفي أنحاء العالم أخذ محترفو الأمن والقراصنة على حدٍّ سواء يتساءلون عمن سيخترق ما لا يُخترق وكم من الوقت سيتطلب ذلك. وكان الجواب هو نادي كاؤوس للحاسب في ألمانيا الذي استغرقه الأمر يوماً واحداً. فباستخدام كلٍ من التمويل الجماهيري والتلعيب، أعدّ القراصنة موقع ويب سموه IsTouchIDHackedYet.com وعرضوا فيه جائزةً بقيمة عشرين ألف دولار تُجمع من تبرعات قراصنةٍ زملاء للنادي، وأعدوا لوحة تحكم تظهر التقدم المتحقق باتجاه هدف العشرين ألف التي أرادوا جمعها. وفي النهاية ذهبت الجائزة إلى قرصانٍ يدعى ستاربَغ من نادي كاؤوس للحاسب، أدرك بذكاءٍ كيف يقهر استثمار أبل الذي بلغت قيمته عدة ملايين من الدولارات. حيث قام ستاربَغ بأخذ صورةٍ عالية الدقة بدقة 2400 نقطة في البوصة لزيوت البصمة التي يتركها صاحب الجهاز الأصلي على شاشة الجهاز. ثم استورد الصورة في برنامج الفوتوشوب ونظفها وقلبها وطبعها على شريطٍ شفاف باستخدام إعدادات طابعة سميكة. وفي النهاية تم دهن الشرط بغراء خشبٍ أبيض فوق الرسم ليجفّ، وعندها صار من الممكن وضعه على حسّاس البصمة لفتح الهاتف، وبذلك أنجزت المهمة.

وكأن جدية قراصنة التمويل الجماهيري لم تكن كافية، ظهرت مؤخراً مشاريع تمويل جماهيري أخرى في الأوساط السريّة الرقمية: سوق الاغتيال. وليست هذه الخدمة، مع الأسف، نوعاً من المزحة الثقيلة، بل هي نتيجة عملٍ شخص فوضوي مخلص يتحرك تحت اسمه المستعار كواباتيك سانجورو. ففي نهاية عام 2014، كان ثمانية مسؤولين حكوميين أميركيين قد اختيروا عبر التصويت بالتعهيد الجماهيري لاغتيالهم. وكان الرئيس السابق للاحتياطي الاتحادي بن برنانك قد تلقى أعلى عددٍ من الأصوات. وكان التبرع يتم باستخدام عملات شبكية مشفرّة غير قابلة للتعقب، وقد تمكن

سانجورو من جمع 75 ألف دولار لاغتيال المدير الاتحادي السابق تُدفع لأي قاتلٍ مأجور يتقدم ويتعهد بتنفيذ المهمة.

مع أنّ مبلغ الـ 75 ألف دولار الذي تم جمعه يدعو إلى الذعر، فإنّه لا يقارن أبداً بعملية التمويل الجماهيري الإجرامية الأكثر نجاحاً على الإطلاق، والتي لم يكن يعلم أحد من المشاركين فيها بطبيعتها. ففي تلك الغارة التي ربما كانت أكثر عمليات السطو التي تقوم بها شركة الجريمة إتقاناً على الإطلاق، استخدم اللصوص في أنحاء العالم التعهيد الجماهيري لتخطيط عملية سطو في 27 بلداً مستقلاً تم تنفيذها بالتزامن. وتمت عملية الاحتيال هذه في بداية عام 2013، عندما قام المبرمجون والمهندسون وعناصر قسم البحث والتطوير في شركة الجريمة في أوروبا الشرقيّة، بالدخول عنوةً إلى شبكتين لمعالجة مناقلات البطاقات الائتمانية في الهند وفي الإمارات العربية المتحدة. وقامت شركة الجريمة بسرقة أرقام بطاقات ماستركارد المسبقة الدفع وبطاقات فيزا، ثم اخترقت نظم الحاسب الداخلية في شبكات المعالجة لإزالة أية قيود على مقادير السحب للبطاقات المسروقة. وكانت النتيجة هي حصول المجرمين المحترفين على المئات من البطاقات الائتمانية تستطيع كل منها سحب مبالغ غير محدودة من شبكة الصرافات الآليّة العالمية.

ثم قامت شركة الجريمة بإرسال رسائل مشفّرة عبر الأوساط السريّة الرقمية إلى شركائها في الجريمة في أكثر من عشرين بلداً. وراح أولئك الذين يتسلمون البيانات المسروقة يستخدمون طابعات البطاقات الائتمانية الاحترافية الإجرامية التي يمتلكونها لطباعة البطاقات الائتمانية وتشفير أرقام البطاقة على الشرائح المغناطيسية على ظهر البطاقة. أما ما حدث بعد ذلك، فكان أحد أعظم الانتصارات للتعهيد الإجرامي، بل وللتعهيد الجماهيري ككل، في التاريخ. حيث تم توزيع البطاقات على مئات الفرق

من النحلات العاملة الإجرامية في أنحاء العالم. وحين أعطت شركة الجريمة الإشارة، بدأ السباق وانطلقت حشود الجنود الخارجة على القانون في عملية سحبٍ خاطفة متزامنة لإصابة أكبر عدد من الصرافات الآلية يمكن للبشر الوصول إليه. وخلال الساعات العشر التي جرت خلالها عملية التعهيد الجماهيري الإجرامية، أجرى اللصوص 36 ألف مناقلة عبر الصرافات الآليّة في 27 بلداً، وغادروا المكان حاملين 45 مليون دولار نقداً. وبما أن شركة الجريمة قد قامت قبل ذلك بالسيطرة على حواسب المصارف، وكانت تعلم ما هي أرقام البطاقات التي تم توزيعها، فقد كانت قادرةً على مراقبة المبالغ المسحوبة بدقة، إضافةً إلى المبلغ الذي يقوم بسحبه كل مجرمٍ عامل، وهو الأهم، وكم عليه أن يعيد إليها بعد حساب "أتعابه". وعلى الرغم من إلقاء القبض على حفنة من العصابات المتدنية المستوى من قبل الشرطة، فإنّ العقول المدبرة التي كانت تقف وراء هذا الهجوم في شركة الجريمة ظلت غير معروفة، وبقيت حرةً طليقة ربما تخطط لهجومها الكبير التالي باستخدام التعهيد الجماهيري. عشر ساعات، 36 ألف مناقلة، 27 بلداً: إنه إنجاز لوجستي مدهش، قليلةٌ هي الشركات أو حتى الحكومات التي تستطيع تحقيقه. إنه عالم الجريمة الموزعة على الشبكات يرحب بكم.

شركة الجريمة هي نشاطٌ تجاري، ونشاط تجاري رابح جداً. وهي لكونها غير مثقلة بالاعتبارات الأخلاقية، تمتاز بحريةٍ لتحقيق الربح دون قيود وباستخدام آخر ما توصل إليه مجال الأعمال. فشركة الجريمة تستخدم سياسات تسعير الفريميوم والتلعيب والتعهيد الجماهيري والتمويل الجماهيري ومحركات السمعة والتصنيع الفوري والتدريب عبر الإنترنت، والأسراب لتنفيذ إدارة المشاريع الموزعة سعياً للوصول إلى الرتل الطويل من ضحايا الجريمة في أنحاء العالم. وقد حققت النقابات الإجرامية العالمية مثل إنّوفيتف ماركتنغ في كييف ما يصل إلى نصف مليار دولار (من دون ضرائب

بالطبع) خلال ثلاث سنوات فقط. هؤلاء الخارجون على القانون، الذين ينطبق عليهم قانون مور، في غاية التواصل وقادرون على استغلال أو قهر أية تقانةٍ إذا ما أرادوا ذلك. وهم يقومون بذلك من دون عقابٍ تقريباً، وأفعالهم تعرض للخطر عالماً يزداد تواصلاً من ناحية ويزداد اعتماداً على التقانة في عمله من ناحيةٍ أخرى. والنتيجة هي وسط إجرامي سرّي أكثر قوة ينمو أسّياً في قدراته. هذه المتعضيّة الإجرامية المتفوقة المزدهرة تعيش وتتنفس ويتم التحكم بها في أعمق مخابئ الإنترنت وأكثرها ظلمة: الويب المظلم، الملجأ الخفي للأوساط السريّة الرقميّة والمركز العصبي لشركة الجريمة.

الفصل الحادي عشر
داخل العالم الرقمي السري

ربما كان تصورنا للمجرم النموذجي مبنياً على خصائص أولئك الأقل ذكاءً الذين تم الإمساك بهم.

نسيم نيكولاس طالب، البجعة السوداء

يعتبر القرصان روبرتس الرهيب (DPR) المطلوب الأول في الأوساط الرقمية السرية. وكان هذا الخارج على القانون يدير إمبراطورية واسعة للجريمة السرية من أكثر أعماق الفضاء السايبري ظلمةً. وقد كان ملاحقاً عالمياً يطارده بدأب مكتب التحقيقات الفيدرالي ووكالة مكافحة المخدرات، والمكتب الفيدرالي للكحول والتبغ والأسلحة النارية والأمن القومي، وشرطة الخيّالة الملكية الكندية والشرطة البريطانية والبوليس الدولي. ولم يكن يعرف عن القرصان روبرتس الرهيب سوى القليل الثمين، كحقيقة أن اسمه المستعار كان مـأخوذاً من شخصية في الفيلم الكلاسيكي الشهير الأميرة العروس، وأنه هو العقل المدبر لطريق الحرير، السوق الإجرامية الهائلة على الإنترنت، والمخفية بعناية عن العامة، والتي كانت تباع فيها جميع أنواع السلع غير المشروعة ضمن شبكة سرية. "إذا كنت تستطيع تدخينه، أو حقنه، أو استنشاقه، فهناك فرصة جيدة لأن يكون موجوداً في طريق الحرير".

كان طريق الحرير، المسمى تيمناً بخط التجارة الآسيوي القديم، مكاناً يمكن فيه للبائع والشاري الالتقاء دون كشف هويتاهما الحقيقيتين ليتبادلا البضائع والخدمات في سوق كبيرة مذهلة للممنوعات. ويقدم طريق الحرير، المعروف بـ إيباي المخدرات والرذيلة، كل المنتجات غير المشروعة الممكن تخيلها منظمة بدقة حسب الفئة، كالمخدرات أو الأسلحة، ومرفقة بالصور والأوصاف. ومن بين السلع المعروضة الأخرى حسابات بنكية

مسروقة، وعملات مزورة، وبنادق كلاشنكوف، وذخائر خارقة للدروع، وبطاقات ائتمان مسروقة، وفيروسات حاسوبية، وبرامج تلصص، وحسابات فايسبوك مخترقة، ودروس تعليمية لاختراق ماكينات الصراف الآلي، ومواد إباحية فيها أطفال، بل حتى قتلة مأجورون يمكن التعاقد معهم. وتحت بند التزوير، كان هنالك أكثر من مئتي عرض لرخص قيادة مزورة، وجوازات سفر، وبطاقات ضمان اجتماعي، وفواتير مياه وكهرباء، بيانات بطاقات ائتمانية، وشهادات جامعية ووثائق هوية أخرى.

لكن طريق الحرير في جوهره ليس سوقاً للمخدرات تحتوي أكثر من ثلاثة عشر ألف مشاركة للمواد الخاضعة للرقابة معروضة للبيع. وتتضمن "قائمة المخدرات" المعروضة للبيع الهيروين، الأوكسيكونتين، مسحوق الكوكايين والمورفين، وثنائي إيثيل أميد حمض الليسرجيك (مهلوس)، عقار النشوة، عقار مولي، الماريغوانا، والكريستال ميث، الفطر المخدر، الحقن، مركبات كيميائية مساعدة، المنشطات، ومجموعة كبيرة من الحبوب التي تتطلب وصفة طبية، من الأديرال وحتى إكساناكس. تباع هذه المواد المخدرة ليس فقط بكميات الاستخدام الشخصي بل وبشحنات كبيرة أيضاً، كعروض بعدة كيلوغرامات من الهيروين، والكوكايين، والميثامفيتامين. وبالنقر على أي رابط، تظهر صورة للمنتج المطلوب مع وصف إعلاني مثل "كوكايين القطران الأسود من نود، يشحن العذوبة في الشرايين، أو في الرئتين إذا كنت تفضل تدخينه ثم مطاردة التنين!".

كان القرصان روبرتس الرهيب يدير على مدى حوالى السنوات الثلاث، أكبر سوق إجرامية على شبكة الإنترنت في العالم، نجح بواسطتها في جذب حوالى 950000 مستخدم فتحوا حسابات على طريق الحرير. ولكن كيف يمكن أن يستمر خرق فاضح للقانون لمثل هذه الفترة الزمنية الطويلة دون أي تدخل فعّال من الشرطة؟ والجواب بسيط، إذ لم تكن لديهم أية فكرة

عن كيفية إيقافه، إذ لم يكن طريق الحرير موقعاً إلكترونياً عادياً يمكن الوصول إليه بكتابة www. ثم اسم الموقع في شريط عناوين متصفح الإنترنت. بل كان طريق الحرير يعمل في الأوساط الرقمية السرية متخفياً وراء جدران من السرية تم الوصول إليها عن طريق استخدام برنامج خاص للتشفير وفك التشفير يعرف بالموجه البصلي، أو تور اختصاراً (سنرى المزيد حول ذلك لاحقاً). باستخدام برنامج تور، يبقى جميع المشتركين من بائعين ومشترين للبضائع غير المشروعة مجهولي الهوية، فيعرفون عن أنفسهم فقط من خلال أسماء مستعارة. ولمزيد من حماية المستخدمين ونشاطاتهم الخارجة على القانون، فإن الطريقة الوحيدة المقبولة للدفع في طريق الحرير هي البيتكوين، وهي عبارة عن نوع جديد من العملة الإلكترونية تسمح للمشتركين بتبادل المبالغ بشكل رقمي وبحماية قوية للخصوصية.

يدرك العارفون بأن اللقب الشائع لطريق الحرير المعروف بـ "إيباي المخدرات" لقب دقيق للغاية. فقد تمكن روبرتس الرهيب، عبر مواكبة التقنيات الجديدة في عالم الجريمة المنظمة، من تأسيس نظام سمعة رقمية متين يمكن المستخدمين من تقييم بعضهم البعض وتقدير مدى الثقة قبل إجراء المناقلة. نعم! يمكنك تقييم مورد المخدرات الذي يورّد لك! وبالتالي فإن Basehead888 قد يرى أن DealioInThe312 قد أنجز أكثر من أربعة آلاف وستمئة صفقة بيع للكوكايين، وهو حاصل على 97 بالمئة على قبول الزبائن من خلال تقييم معجبيه المخدَّرين المغرمين به. كما يمكن قراءة تعليقات محددة من الزبائن تصف "كم كان توصيل البضاعة سريعاً"، أو "كم كان التغليف قوياً لا يمكن حتى للكلب المدرب على تشمم المخدرات شم أي شيء".

نمت مع مرور الوقت شعبية وشهرة طريق الحرير، وفي زمن قصير بات يتم تبادل ما يقرب من 600,000 رسالة خاصة شهرياً بين البائعين

والمشترين، وفي النهاية أصبح حجم التبادل والتحويل أكبر من أن يستطيع القرصان روبرتس الرهيب وحده التعامل معه. لذلك عين الزعيم المجرم طاقماً صغيراً من المشرفين على النظام، حيث كان واحدهم يتقاضى 1000 إلى 2000 دولار في الشهر، وذلك لقاء المساعدة في تسيير العمليات اليومية على الموقع، بما في ذلك مراقبة نشاط المستخدمين تجنباً للمشاكل، وكذلك تأدية خدمات الزبائن، والتواسط بين المشترين والبائعين حيث يوجد نزاع.

لكن المؤسس لأكبر سوق سرية للبضائع غير الشرعية في العالم، كان يجني بالطبع أكثر بكثير من موظفيه، الأمر الذي سرعان ما لاحظه المشرفون الأقل مستوى. وهكذا، وللتعامل مع الظلم الواقع عليه مع هذا الراتب المنخفض، بدأ أحد موظفي طريق الحرير بالاختلاس من الشركة. لكن أي شخص شاهد فيلم سكارفييس (الوجه ذو الندبة)، أو فيلم السوبرانو، أو فيلم العراب أن يخبرك أن السرقة من الزعيم هي فكرة سيئة دائماً. فحين لاحظ القرصان روبرتس الرهيب أنه كان يتعرض للسرقة، اعتبرها خيانة لا يمكن أن تغتفر، ورداًّ على ذلك قام بالاتصال بأحد القتلة المأجورين المحترفين على الموقع للتفاوض على تصفية الموظف مقابل 80,000 دولار (خمسون بالمئة مقدماً للاغتيال تبعاً لشرط التعاقد). كان روبرتس الرهيب غاضباً للغاية من الإهانة التي تعرض لها من قبل موظفه، لذلك طلب من القاتل المأجور تعذيب موظفه قبل قتله. أرسل روبرتس إلى القاتل المأجور عنوان الموظف في ولاية يوتاه، وقبل بأن يدفع المبلغ المتبقي المتفق عليه بعد رؤية دليل بالصور الفوتوغرافية على عملية القتل. وبعد عدة أيام تلقى المدير التنفيذي لطريق الحرير الدليل الذي كان يريده على هيئة صورة رقمية، فقام روبرتس، الذي يفي بكلامه، بتحويل مبلغ 40,000 دولار للقاتل، حتى إنه أرسل له رسالة شكر على القيام بالمهمة متباكياً في رسالة إلكترونية مشفرة: "أنا منزعج جداً أنه كان عليّ قتله... ولكن ما حصل قد حصل... لا

أستطيع أن أصدق كم كان غبياً... كنت أتمنى فقط أن يتحلى المزيد من الناس ببعض النزاهة". نعم! إن مؤسس طريق الحرير، أكبر سوق عالمية للبضائع غير المشروعة، والذي أمر للتو بقتل أحد موظفيه، كان منزعجاً من نقص النزاهة في هذا العالم!

لكن هذه المرة لم تكن المرة الوحيدة التي يأمر فيها روبرتس الرهيب بتصفية شخص قام بالتجاوز عليه، فقد كانت مآثره سراً مكشوفاً في الأوساط الرقمية السرية، حتى إن مجلس الشيوخ الأميركي عقد جلسات استماع مطالباً الشرطة بالتدخل. وكان مكتب التحقيقات الفيدرالي وآخرون قد انكبوا على القضية مسبقاً بالطبع، وقاموا بأكثر من مئة عملية شراء سرية على الموقع. ولم يمض وقت طويل حتى كانوا في أثر عراب طريق الحرير، مقاول الإنترنت، سيد المخدرات القاتل الذي بدأ كل شيء. وقادت عملية المطاردة العالمية للقرصان روبرتس الرهيب أخيراً فرقة طريق الحرير في مكتب التحقيقات الفيدرالي إلى فرع غلين بارك لمكتبة سان فرانسيسكو العامة.

هناك، وفي يوم مشمس لطيف في خريف عام 2013، كان رجل في أواخر العشرينيات ذو شعر بني متماوج، يجلس مع حاسبه المحمول بهدوء في قسم الخيال العلمي، يكتب على الحاسب بينما المحيطون به يقرأون لكتبهم ويتصفحون مجلاتهم. وفجأة كُسر الصمت حين تقدمت شابة من الرجل الشاب صائحةً "لقد سئمت منك!" وفي لحظة أصبحت فوقه وانتزعت الحاسب المحمول من الطاولة. وحين صارع لاستعادة الحاسب، قام جالسون على طاولته بدلاً من مساعدته بدفعه تجاه الحائط، سامحين للشابة الغريبة بالهروب بأغلى ما يملك.

لم تكن هذه عملية سرقة عشوائية، فقد كان الكثير من هؤلاء المتنكرين كعشاق للكتب ينتظرون بفارغ الصبر هذا الشاب العشريني وحاسبه

المحمول. وحالما شغل الشاب حاسبه وأدخل كلمات السر اللازمة لفك تشفير القرص الصلب انقضّ المهاجمون، لكن المواجهة لم تدم طويلاً، وانتهت في لحظة حين أشهر المهاجمون شارات مكتب التحقيقات الفيدرالي، كاشفين عن هويتهم. وراح عاملو المكتبة المذهولون يراقبون فاغري الأفواه عملية القبض على الشاب ذي الشعر البني المتماوج وأخذه إلى سجن غلين دير في أوكلاند حيث سيتم توقيفه. لقد أصبح القرصان روبرتس الرهيب شيئاً من الماضي!

على الرغم من قيام روبرتس الرهيب بجهد كبير لحماية هويته من خلال استخدام تور والعملة الإلكترونية (بيتكوين) لتغطية أثره، فإنه ارتكب سلسلة من الأخطاء التشغيلية المتراكمة قادت في النهاية الشرطة الفيدرالية إلى تسجيلاته المتكررة للدخول في مكتبة سان فرانسيسكو العامة. ووفقاً للاتهام الفيدرالي، فإن القرصان روبرتس الرهيب هو في الحقيقة روس ويليام ألبريشت، ذو التسعة والعشرين من ولاية تكساس الذي انتقل للعيش في سان فرانسيسكو منذ بضعة أعوام.

اتهم المدعي العام للمنطقة الجنوبية من نيويورك ألبريشت، المعروف بالقرصان روبرتس الرهيب، بجملة من الاتهامات من ضمنها "التآمر للقيام بتهريب المخدرات، واختراق أنظمة الحاسب، وغسيل الأموال، وإدارة منظمة إجرامية"، أجل، لقد تم اتهام ألبريشت أيضاً بمحاولة القتل و"استخدام مرافق التجارة بين الولايات للتعاقد على القتل المأجور". وتبين لاحقاً أن القاتل المأجور الذي ظن روبرتس الرهيب أنه قد استأجره، كان عميلاً فدرالياً متخفياً. واتهمت النيابة العامة ألبريشت أيضاً بإعطاء الأوامر لخمس عمليات قتل أخرى. فحين قام ألبريشت بدفع المبالغ المطلوبة إلى القتلة المفترضين، تأكد لمكتب التحقيقات الفيدرالي من أنه جدي للغاية وتدخّل لإنقاذ المستهدفين، حيث تمكنت الشرطة الفيدرالية من الاعتماد

على تعاون جميع المستهدفين بالقتل، وأخذت صوراً ملفقة للضحايا المزعومين وهم يضعون مكياج يبدون فيه كالجثث، لتُرسل إلى روبرتس الرهيب كدليل على عمليات القتل التي أمر بها.

فمن هو هذا العقل الإجرامي المدبر الذي يقف وراء طريق الحرير؟ إنه ليس إطلاقاً ما يمكن أن تتوقع منه. روس ألبريشت كان ولداً يفخر به أي والدين. عضو في كشافة النسر في أوستن، تكساس، وحاصل على شهادة الماجستير في العلوم والهندسة. خلال دراساته العليا، فقد ألبريشت أخيراً الاهتمام بالعلم لحساب شغف جديد للتحررية. وكتب على صفحة حسابه في موقع لينكدإن، أنه يتمنى "استخدام النظرية الاقتصادية لإلغاء الاستخدام الواسع النطاق والمنهجي للقوة من جانب المؤسسات والحكومة ضد البشرية". في تلك اللحظة بالذات ولد القرصان روبرتس الرهيب، وأصبح طريق الحرير اللوحة التي يمكنه عليها تجريب وتحسين الحدود التي يراها مثالية للسوق الحرة. لكن النتيجة، كما في مسلسل والتر وايت التلفزيوني Breaking Bad fame، هي قصة واقعية لعالم حوّل شغفه للمخدرات والفوضوية التشفيرية إلى أكبر مورد إنترنت للممنوعات في العالم. ومن خلال ذلك كسب هذا الخارج على القانون ثروة طائلة.

على غرار موقع إيباي، كان طريق الحرير يقتطع عمولة عن كل عملية بيع تتراوح بين 8 إلى 15 بالمئة وفقاً لحجم العملية. ووفقاً للائحة الاتهام ضد ألريشت، فقد عالج طريق الحرير عمليات تحويل بأكثر من 1.2 مليار دولار في الفترة الممتدة بين شباط 2011 وتموز 2013 فقط! محققاً صافي ربح مذهلاً للمؤسس ذي التسعة والعشرين يقدر بـ 80 مليون دولار كعمولة. ليس هذا مبلغاً سيئاً بالنسبة لشركة ناشئة خلال عامين. في ذروة عملياته، وتبعاً لدراسة نشرت في جريدة أديكشن (الإدمان)، فإن ما يقارب العشرين بالمئة من متعاطي المخدرات في الولايات المتحدة سبق لهم أن

اشتروا مخدرات على موقع طريق الحرير.

رد ألبريشت على الاتهامات بأنه بريء منها جميعاً، وقد صرحت عائلته وأصدقاؤه بإصرار بأنه "شخص لطيف جداً"، حتى إنهم أطلقو حملة جمع تبرعات لمساعدته على دفع أجور المحاكمة (العملة الإلكترونية مرحب بها). أما الحكومة الفدرالية فكانت من جهتها ترسم لألبريشت صورة أقل دماثة بكثير في لائحة الاتهام المقدمة من قبلها، صورة لسمسار مخدرات، وقاتل بدم بارد، وعقل إجرامي مدبر اخترع نموذج الجريمة المنظمة من جديد. سواء أكان ألبريشت من نسور الكشافة أم شريراً، ثمة أمر واحد واضح، لقد أضاف ألبريشت المدعو بالقرصان روبرتس الرهيب لقباً جديداً لقائمة أسمائه الطويلة، وهو النزيل ULW981 المحبوس في زنزانة لمدة عشرين ساعة في اليوم ويواجه عقوبة بالسجن مدى الحياة. في الوقت ذاته، وكما الهيدرا المتعددة الرؤوس، عاد طريق الحرير إلى الحياة بعد أن توقف لفترة قصيرة، وذلك تحت إدارة جديدة، ليزدهر ازدهاراً واسعاً في كواليس الويب المظلمة الواسعة التي تمثل الأوساط الرقمية السرية.

جواز سفر إلى الشبكة المظلمة

كان على البائعين والمشترين المجرمين الراغبين بالإتجار في طريق الحرير الذي أسسه روبرتس الرهيب، معرفة كيفية الوصول إليه أولاً. فكما في العالم الواقعي، لا يمكنك أن تطرق باباً لا على التعيين في مبنىً ما متوقعاً الحصول على كيلو من الميثامفيتامين. وينطبق الأمر نفسه على الأوساط الرقمية السرية، إذ لا يمكنك الوصول إليها بمجرد كتابة عنوان لموقع في متصفح فايرفوكس متمنياً حصول المعجزة بأن تفتح في وجهك غياهب عالم الجريمة المنظمة، بل ستحتاج إلى جواز للمرور وإلى دليل لإرشادك. وتبدأ الرحلة مع موجّه تور (موجه البصل)، وهو برنامج حاسوبي يعمل كأداة توفر أقصى حد ممكن من إغفال الهوية على شبكة الإنترنت.

يعمل تور على إعادة توجيه اتصالاتك بالإنترنت، عبر مجموعة من خمسة آلاف مخدم منتشرة حول العالم بغرض إخفاء مصدر وهدف الاتصال. فمن بدون تور يسهل تعقب نشاطاتك على الشبكة، ففي كل مرة تزور فيها موقع سي.إن.إن أو إي.إس.بي.إن، تكشف موقعك وعن شبكتك المنزلية، الأمر الذي لا يعجب المجرمين لأنه يسمح بالقبض عليهم. لذا فإنهم يقومون بالتغطية عبر تحويل نشاطهم على الشبكة عبر خدمة مثل تور، بحيث لا تتمكن الشرطة من رؤية أفراد العصابات يبيعون بنادق الكلاشنيكوف على الشبكة من خلال مخدم كومكاست في شيكاغو (الذي يكفي أن يتعرف على رقم إنترنت زائره حتى يتم إصدار مذكرة إحضار بحقه). عوضاً عن ذلك يقوم أي قرصان متمرّس، ولنقل أنه في موسكو، بتوجيه تنقلاته في الإنترنت عبر لندن ثم كيب تاون ثم طوكيو ثم أوستن، فميلان قبل أن يظهر لمهاجمة هدفه في مانهاتن، ما يجعل هذه "المكالمة" مستحيلة التعقب تقريباً.

ورغم أن تطبيق تور Tor البرمجي يمكن استخدامه لإخفاء الهوية لدى زيارة موقع إلكتروني عادي كغوغل مثلاً، فإن قوته الحقيقية تكمن في تمكينه من الاتصال بمواقع تخديم تور المخفية، المعدة خصيصاً لتلقي الاتصالات الواردة من خلال شبكة تور. ببساطة لا يمكن الوصول إلى المحتوى الواسع المتوافر بشكل مخفي في الشبكة دون تطبيق تور البرمجي. وباستخدام هذه الخدمات المخفية لتور، يمكنك ليس فقط إخفاء هوية الزائر، بل وحماية خصوصية الموقع المخفي أيضاً، فبدلاً من استخدام عنوان إنترنت عادي كعنوان فايسبوك Facebook.com مثلاً، تستخدم جميع خدمات تور المخفية أسماءها الخاصة لنطاق الشبكة، والذي ينتهي بلاحقة) (بصل). يسمح هذا النظام المزدوج لإخفاء الهوية لكلٍّ من البائع والمشتري على طريق الحرير بالتعامل مع بعضهما من خلال زيارة نطاق خاص على

الشبكة (في حالة طريق الحرير silkroadvb5piz3r.onion) من خلال تطبيق تور الذي يضمن لهما عدم كشف هويتهما أحدهما للآخر.

على الرغم من أن معظم الناس لم يروا أو يستخدموا تطبيق تور البرمجي، فإنه متاح مجاناً للتحميل من خلال موقع www.torproject.org. ويمكن تنصيبه خلال دقائق قليلة، وتشغيله بشكل مخفي لينقل المستخدمين بشكل فعال من نطاق شبكة المعلومات الرئيسية. وللمفارقة، فقد تم تصميم وتمويل تور كمشروع لمختبر الأبحاث البحرية الأميركي في عام 2004، وبدعم من مؤسسة الريادة الإلكترونية ووزارة الخارجية وذلك لمساعدة المنشقين وناشطي الديمقراطية المنشقين عبر البحار على تنظيم أنفسهم والتواصل بين بعضهم البعض بأمان. وهنالك عدد كبير من الاستخدامات الشرعية لتور، فأولئك الموجودون خلف جدران المنع الكبيرة في الصين وإيران ومناطق أخرى، يعتمدون بشكل منظّم على تور للوصول إلى كل شيء من الفايسبوك إلى جريدة النيويورك تايمز. كما أن استخدام تور يتزايد من قبل الصحافيين للتواصل مع مصادر معلوماتهم ومع كاشفي الفساد بأمان، كأولئك العاملين في مجموعات ويكيليكس.

فيما أن تور قد تم إنشاؤه لأهداف خيّرة، فإن قدرته الكبيرة على تسهيل عملية التواصل السرية دفعت المجرمين، الأمر الذي لا يمثل مفاجأة، إلى تبنيه على نطاق واسع، وهو ما مكنهم من خلق خدمات كطريق الحرير. ورغم أنه من غير الممكن على وجه الدقة تحديد عددها، فإن دراسة عام 2 غطت أربعين ألفاً من مواقع تور المخفية، وجدت أن 50 بالمئة منها تقريباً متورط في أعمال غير شرعية كبيع بطاقات الائتمان المسروقة والحسابات المخترقة والأسلحة والمخدرات والمواد الإباحية المتضمنة للأطفال. يقدر بعض خبراء الأمن والقانون بشكل غير معلن، أن 85 بالمئة من خدمات تور المخفية هي أعمال خارجة على القانون، حيث يتجاوز معدل الاستخدام

الإجرامي إلى حدّ كبير معدل استخدام ناشطي الخصوصية.

حتى بداية عام 2014، تم تحميل برنامج تور حوالى 150 مليون مرة ليتم استخدامه يومياً من قبل مليوني شخص. وبافتراض أن الاستخدام غير الشرعي يمثل النسبة المتحفظة البالغة خمسين بالمئة، فإن ذلك يعني أن 300,000 مجرم يستيقظون يومياً ويذهبون للعمل على الشبكة الرقمية السرية باستخدام خدمات تور المخفية. ويبين لنا قانون ميتكالف، الذي يعتبر أن قيمة شبكة الاتصالات تتناسب طرداً مع مربع عدد المستخدمين المتصلين بالنظام، حجم التهديد الذي تفرضه مجموعة متشابكة ومتصلة من المجرمين مغفلي الهوية.

ربما لا تكون شركة الجريمة هي القوة الشريرة الوحيدة التي تستخدم تور للوصول إلى خدمات الشبكة السرية، فقد ورد في بعض التقارير، أن تنظيم القاعدة وشركاءه كانوا يستفيدون أيضاً من ميزات السرية وإغفال الهوية التي يوفرها استخدام برتوكول تور المشفر، للاتصال في تجنيد العملاء الجدد وجمع التبرعات ونشر الدعاية، بل وحتى التخطيط للهجمات. فبعد أن سرّب المتعاقد مع وكالة الأمن القومي إدوارد سنودن تفاصيل قدرات وكالته الواسعة في اعتراض الاتصالات، ظهرت دلائل تشير إلى إعادة تقييم العديد من المجموعات الإرهابية لاستراتيجيات الاتصال التي تتبعها، وراحت تشدد في الكثير من خطاباتها لأعضائها على أهمية الأمن العملياتي الدائم على شبكة الإنترنت.

بل إن منظمات كالقاعدة في شبه جزيرة العرب وأنصار المجاهدين، قامت بإنتاج مواد تدريبية وفيديوهات على اليوتيوب لتشجيع أعضائها على استخدام تور في جميع نشاطاتهم على الشبكة.

بالنظر إلى تسريبات سنودن، وكذلك الاعتداءات الواسعة على الخصوصية الملاحظة سابقاً، فإنه من المنطقي تماماً أن يلجأ المواطنون العاديون إلى أداة

فعالة كتور للحفاظ على كرامتهم وحريتهم وحقوقهم الأخرى على الإنترنت. لكن رغم ذلك فإن سيطرة شركة الجريمة على خدمات تور المخفية وابتكاراتها التي لا تزال تطلقها في الأوساط الرقمية السرية تثير العجب نظراً لحجمها ومداها وأبعادها.

رحلة إلى الهاوية

تقوم الإنترنت بتزويد الحالات العقلية المرضية بنظام تسليم وتوزيع.
فيليب آدامز، مذيع وكاتب أسترالي

ربما كنت تظن أنك تعرف الإنترنت حق المعرفة، لكنك مخطئ. فبينما تتجول فيها يوماً بعد يوم لتشاهد الفيديوهات على اليوتيوب وتنشر تحديثات حالتك على الفايسبوك وتتسوق على أمازون، ربما تتخيل أنك في جنة عدن الإنترنتية، لكن الأمر ليس كذلك. فمنذ اللحظة الأولى التي دخلت فيها إلى عالم الإنترنت وحتى الآن لم تزر الشبكة السطحية للإنترنت فقط، فقد تمت محاصرتك بين جدران حديقة مُسوَّرة مصممة ومشذبة بعناية فقط من أجلك، بينما دخل العارفون شبكة الماتريكس، العالم الرقمي الآخر. هذه هي شبكة الإنترنت التي لن يراها معظمنا، وهي تسمى بأسماء عديدة منها شبكة الويب العميقة أو الشبكة المظلمة أو السرية، أو الأوساط الرقمية السرية، أو الإنترنت غير المرئي. إنها إنترنت الظل التي لن يأخذك إليها غوغل.

يُقصد بشبكة الوب العميقة تقنياً مصادر المعلومات على الشبكة التي لا يمكن لمحركات البحث كغوغل وياهو وبينغ فهرستها، وذلك لأنها محمية بكلمات مرور أو تستوجب دفع المال أو تتطلب برامج دخول خاصة. ولأن محرك غوغل المتطور للبحث في محتوى الإنترنت لا يستطيع الكتابة أو إدخال كلمات المرور أو إكمال عبارات التحميل (الكابتشا) أو التسجيل في مواقع خاصة، فإنه يعجز عن فهرسة واحتواء مساحات هائلة من

المعلومات في العالم. ينتظم الكثير من محتوى الشبكة العميقة غير المفهرس في قواعد البيانات الأكاديمية مثل ليكسيس نيكسيس، أو في مجموعات البيانات المبوبة بحسب المواضيع كتلك الموجودة في مكتب براءات الاختراع، أو مكتب الإحصاء. لكن إضافة إلى هذا المحتوى العادي، يوجد الكثير من المواد البذيئة.

من الصادم أن تكون شبكة الوب العميقة أكبر بخمسمئة مرة من الشبكة السطحية التي تستخدمها وتبحث فيها يومياً. فبينما تحتوي الشبكة العميقة على سبعة آلاف وخمسمئة تيرابايت من المعلومات، يحتوي العالم الذي يمكن البحث فيه عبر غوغل على حجم تافه يبلغ تسعة عشر تيرابايت. ووفقاً لدراسة أجرتها مجلة نيتشر فإن غوغل يفهرس ما لا يزيد على 16 بالمئة من شبكة الويب السطحية وغير قادر على فهرسة أي شيء من الشبكة العميقة. لذلك فإنك حين تستخدم غوغل للبحث فإنك تشاهد 0.0 بالمئة (واحد من ثلاثة آلاف صفحة) من المعلومات المتوفرة فعلياً والتي كانت ستتاح لك لو كنت تعرف كيفية الوصول إليها. بعبارة أخرى، فإن بحث غوغل يغفل 99 بالمئة من بيانات شبكة الوب العالمية. فالبحث على الشبكة اليوم يماثل صيد السمك حتى عمق قدمين فقط من محيطات العالم الواسعة، فمع أنك قد تصطاد شيئاً ما بشبكتك، لكنك تخسر الجائزة العظيمة المتاحة تحت هذين القدمين وصولاً إلى أعماق البحار. أما أولئك المقدامون، فينتظرهم المعادل الرقمي لخندق مارينا، كنز حقيقي غير مكتشف من البيانات ينتظر أن يُكتشف.

ولكن كلعبة الماتريوشكا الروسية، يُعشش داخل الشبكة العميقة عالم خفي ذو مجتمع أصغر لكنه خطير، يجمع القوى الخبيثة لأجل الهدف المشترك السيّئ. أهلاً بكم في الشبكة المظلمة، العالم الرقمي الخفي داخل الشبكة العميقة الذي يأتي إليه قراصنة الإنترنت وأفراد العصابات

والإرهابيون والبيدوفيليون لعقد صفقاتهم. تستحوذ الشبكة المظلمة على بعض أعظم الأسرار التي يمكن أن تحتويها الإنترنت، وهي أشبه الأزقة الخلفية والأسواق السوداء في أية مدينة كبيرة، ففيها يتواصل المجرمون لممارسة نشاطاتهم غير المشروعة. تستخدم الشبكة المظلمة التشفير وقنوات التقوية المباشرة الزوجية والمصممة خصيصاً لإخفاء عناوين الإنترنت الخاصة بمستخدميها، لتوفر بالتالي منصة آمنة غير قابلة للتعقب وتحافظ على سرية الهوية للجريمة المنظمة للتواصل والتعامل دون الخوف من تدخل الحكومة أو الشركات.

على الرغم من أن تور هو البوابة الأكبر والأكثر شعبية إلى الشبكة المظلمة، فإن لديه منافسين، مثل فرينيت (الشبكة الحرة) وآي.2.بي (مشروع الإنترنت غير المرئي). علاوة على ذلك، ليس طريق الحرير سوى واحد من عشرات الأسواق الإجرامية على الإنترنت، من ضمنها "السوق السوداء الجديدة"، و"السوق المفتوحة"، و"سوق الخراف"، وأجورا، و"البنك الأسود"، وأتلانتس، و"سوق القراصنة"، وقنوات جديدة تظهر وتختفي يومياً. والأهم من ذلك أن المجرمين أشبه برجال أعمال جيدين يتعلمون من أخطائهم السابقة. فعقب إغلاق طريق الحرير، ظهر مكانه جيل جديد من أسواق الشبكة المظلمة، أبرزها "السوق المظلمة"، وبينما كان طريق الحرير مركزي التحكم يسيطر عليه القرصان روبرتس الرهيب من خلال المخدمات التي يديرها، فإن "السوق المظلمة" هي سوق سوداء على الإنترنت لامركزية بالكامل، من دون مالك محدد. ولكي ينجح مكتب التحقيقات الفيدرالي بالقضاء عليها، لن يكفي اعتقال مؤسسها، حيث لا يوجد شخص كهذا. أي إن الشرطة ستضطر إلى ملاحقة كل بائع ومشترٍ للممنوعات واحداً تلو الآخر، وهو أمر شبه مستحيل، الأمر الذي يجعل السوق المظلمة جنة حقيقية للجريمة المنظمة.

لمساعدة المجرمين والمخترقين الجدد على تصفح الشبكة المظلمة، أسست أسواق الممنوعات موسوعات ويكي إجرامية (أشبه بجريميبيديا)، منظمة بعناية حسب الفئة مع وصلات لمواقع onion أخرى. تتضمن هذه القوائم فئات مثل الاختراق والمهووسين بالتقانة والفوضوية والبرامج المقرصنة والفيروسات والأسواق والمخدرات والمواد الإباحية، كلها مع روابط تشعبية وتوصيف لما يوجد تحت كل بند. وحتى مع مساعدة الويكي، فإن تصفح الشبكة المظلمة يشكل تحدياً، ويمكن أن يكون من الصعب إيجاد مخدر محدد أو سلاح ما أو قاتل مأجور ما تقوم بالبحث عنه. لذلك قام أحد القراصنة المبدعين بإيجاد أول محرك بحث للشبكة المظلمة يعرف بغرامز، المستوحى تصميمه من محرك البحث غوغل. ولا يمكن الوصول إلى محرك غرامز سوى عن طريق متصفح تور الذي يغفل الهوية وباستخدام عنوان إنترنت منتهٍ بـ.onion. مع محرك بحث غرامز يمكن لأولئك الباحثين عن الممنوعات إدخال كلمات رئيسية للبحث عن السلع والخدمات، عبر ثماني أسواق سوداء مختلفة بشكل متزامن. يعطي محرك البحث ضمن نتائجه اسم البائع ويسمح بمقارنة النتائج بهدف التسوق. وكما في غوغل، يوفر المحرك زر "ضربة حظ" توجه المستخدم مباشرة إلى شيء من قبيل "كريستال ميث عالي الجودة". بل إن غرامز، الأشبه بنموذج أولي لغوغل في مجال الجريمة، يستقبل الإعلانات ويسمح لعصابات تهريب المخدرات بالتنافس على الزبائن عبر شراء كلمات البحث. أجل، حين تبحث عن "هروين أفغاني بني" في غرامز، فإنه سيرد بسرد جميع النتائج المتوفرة في شبكة الوب المظلمة، لكن نتائج البحث التابعة لشركات الجريمة التي دفعت الرسوم ستوضع في مراتب أعلى ضمن النتائج، تماماً كنتائج البحث المدفوعة في غوغل. ووجود برنامج أدوورد الذي يقدمه غرامز للأوساط السرية الرقمية يبين قدر المعرفة التقنية التجارية المتقدمة والتعقيد الذي

وصلت إليه شركة الجريمة.

مع وصول البحث مع إمكانية الإعلان إلى العالم السري الرقمي، لم يكن جميع المتداولين الإجراميين سعداء بإمكانية الوصول إليهم بهذه السهولة من قبل جماهير المجرمين، وبالتالي من قبل القوى التنفيذية. ففي براري الويب المظلم الأكثر انتقائيّة، كما في العالم الحقيقي، لا بد للمجرمين على الشبكة من التعريف بأنفسهم ومن تقديم كفلاء قبل أن يبدأوا بالتداول. فهنا "يتم توزيع البضائع والخدمات بشكلٍ منظم عبر غرف محادثة غير شرعيّة ومنتديات لا يتم دخولها إلا بدعوة". وللوصول إلى النطاقات المحظورة الأكثر حصريّة، لا بد للمرء من أن يكون مجهّزاً بالعنوان السرّي الأبجدي - الرقمي، ولا يكون هذا العنوان مبوباً أو مُدرجاً في أي مكان على الشبكة، بل يتم تمريره حصراً من شخصٍ إلى آخر. وثمة منتديات إجرامية معينة مثل موقع التجميع الروسي مازا، وهو سوق هائل للبطاقات الائتمانية المسروقة على الإنترنت، لا تقبل الطامحين إلى دخول عوالمها السريّة، إلى أن تتم الموافقة عليهم بالإجماع من قبل أعضاء المنظمة الكبار وانقضاء فترة انتظار تبلغ ثمانية أيام. إلا أنّه ما إن يتم قبولك في مملكة نخبة الأجيال الإجرامية حتى يصبح العالم ملك يديك.

عند استعراض الأعداد الوفيرة من البضائع المحظورة وغير الشرعيّة المتوفرة في العالم السرّي الرقمي، يشعر المرء وكأنه يهبط حلقات غانتي الجهنميّة التسع، تقوده كل خطوةٍ أعمق وأعمق في هاوية مشؤومة لا قرار لها. سنسرد فيما يلي عينة سريعة من البضائع والخدمات المتوفرة في أكثر الجحور ظلمةً في الإنترنت مدرجة من أبسطها إلى أكثر رعباً.

المحتوى المقرصن

ثمة الكثير من مواقع مشاركة الملفات بواسطة الشبكات الزوجية غير الشرعيّة المعروفة بـ-تورنت، مثل خليج القراصنة الذي صُنفّ بين المواقع

المئة الأكثر زيارة على الإنترنت. وثمة موقع ثانٍ هو موقع ميغا أبلود النيوزلندي الذي وصل عدد زائريه في ذروته إلى خمسين مليون "زبون" في اليوم، أي ما يمثل نسبةً تصل إلى 4 بالمئة من حجم النقل عبر الإنترنت كلها على مستوى العالم. وترى السلطات التنفيذية الدولية، أن من يدير الموقع هو قرصان ألماني الجنسية مغترب بطول ست أقدام وسبعة إنشات ووزن 350 باونداً، يستخدم الاسم المستعار كين دوت كوم، ووفقاً للسلطات، فإن المنتجات الأساسية في الموقع هي عبارة عن خمسين بيتابايت (أي 52 مليون غيغابايت) من الأفلام والأغاني وألعاب الفيديو والكتب والبرمجيات المسروقة. كانت الأعمال تسير على ما يرام في الموقع، وكانت الشركة تحقق أرباحاً سنوية تقدر ب25 مليون دولار من الإعلانات على الإنترنت إضافةً إلى 150 مليون دولار هي مجموع الرسوم التي يسددها المستخدمون الراغبون بسرقة المحتويات القابلة للتحميل بسرعةٍ أكبر، وتسمح هذه الأرباح لـ كيم دوتكوم بالاستمتاع بحياةٍ في غاية الترف في قصرٍ تبلغ قيمته 24 مليون دولار مع ستين فداناً من مروج العشب المشذّبة مع ملاعب تنس وغولف خاصّة. ومن بين الممتلكات الأخرى لكيم دوتكوم طائرة مروحية ويختٌ كبير و15 مرسيدس وسيارة روزرايس شبح (إم.إس.إر.بي) بقيمة 4' دولار وسرير من شعر الحصان السويدي ماركة هستنس فُصّل له خصيصاً بتكلفة 103,000 دولار. بالفعل، فإنّ القرصنة مجال أعمال مربح.

المخدرات

كما رأينا مع طريق الحرير، تتوفر العقاقير المحظورة وتلك التي لا تصرف إلا بوصفة طبيب بجميع أنواعها في الأوساط السريّة الرقميّة، وبكمياتٍ تتراوح بين جرعات الاستخدام الشخصي والمبيعات بالجملة بين التجار. لكن طريق الحرير ليس في أي حالٍ من الأحوال سوق المخدرات الوحيدة على الويب المظلم، فثمة المئات من مثل هذه المواقع. وهي لا تبيع المخدرات

النموذجية مثل الماريغوانا والهيروين والاكستازي والكوكائين فقط، بل توفر أيضاً بضائع أكثر ندرة بكثير سكوبولامين، أو ما يعرف بمسحوق الشيطان نفسه الذي يستخدم كعقار قوي للتحول إلى زومبي، إذا ما نُفخ في وجه الضحية تركها متماسكةً لكن فاقدةً للإرادة الحرة. فعندما يتم استنشاقه، يسمح هذا الغبار الذي لا طعم له ولا رائحة للّصوص والسلبة والمغتصبين خلال دقائق بإحكام سيطرتهم تماماً على ضحيتهم. والأسوأ من ذلك أنه يمحو ذكريات الضحية عن جميع تفاصيل الحادثة.

العملة المزوّرة

تتوفر العملة المزوّرة على نطاقٍ واسع في الأوساط السريّة الرقمية، وتختلف تكاليفها تبعاً للجودة والكمية المشتراة ونوع العملة. وتتوفر منها عملات الدولار واليورو والباوند والين وغيرها. وثمة مواقع تتخفى خلف شبكة تور مثل Guttemberg وprint وCheap Euros وWHMX Countert تقدم أوراقاً نقدية عالية الجودة مقابل 24 سنتاً للدولار الواحد، (أي 600 دولار حقيقي لشراء 2500 دولار مزور). ويعد البائعون بأن جميع هذه الأوراق النقدية ستتجاوز اختبارات القلم والأشعّة تحت البنفسجية التي عادةً ما تطبق لكشف العملات المزورة.

البضائع والإلكترونيات الفارهة المسروقة

توفر مواقع الويب المظلم مثل Tor Electronics وCardedStore وButtery Bootlegging إلكترونيات جديدة من ماركاتٍ معروفة وبضائع فارهة، مع تخفيضاتٍ خاصة بالويب العميق. وتروج إعلاناتها لـ "بضائع باهظة الثمن من كبرى المتاجر مقابل جزءٍ زهيد من السعر الأصلي!" وتكون هذه البضائع بالطبع قد سرقت أو سرّبت من المعمل أو اختفت على نحوٍ غامض من شاحنات التوزيع.

البطاقات والحسابات

ربما لا تتوفر سلعةٌ في الأوساط السريّة الرقميّة كما تتوفر البطاقات الائتمانية المسروقة، التي عادت ما توجد فيما يسمى منتديات لصوص البطاقات التي يمكن للأفراد فيها بيع وشراء البطاقات الائتمانية والمدينة من أي مصرفٍ أو بلدٍ في العالم، فجميع البيانات المالية المسروقة بواسطة البرمجيات الخبيثة والاختراق وبرمجيات السطو على البطاقات الائتمانية، تنتهي معروضةً على البيع في شبكة الويب المظلم عبر "المقالب". وتشير كلمة المقالب إلى البيانات المحتواة على الشريط المغناطيسي على البطاقة الائتمانية وتشتمل على جميع التفاصيل، مثل اسم حامل البطاقة ورقم البطاقة وتاريخ انتهاء صلاحيتها وقيمة التحقق الخاصّة بها. فبعد أن تتم سرقتها، تستخدم هذه المعلومات من قبل المجرمين لتسديد المشتريات على الشبكة، بل وحتى طباعة هذه البيانات على بطاقاتٍ بلاستيكية جديدة مزورة يستخدمونها لتسوق "بضائع مُكلفة يمكن إعادة بيعها بسرعة للحصول على السيولة". ونظراً للكميات الكبيرة من البطاقات الائتمانية التي تتم سرقتها، فإن سعر البطاقة المسروقة في الأوساط السريّة الرقميّة لا ينفك يهبط (من 3 دولارات عام 2010 إلى دولارٍ واحد عام 2013). تبيّن مقالب البطاقات الائتمانية المسروقة مرونة هذه السوق. فبعد اقتحامٍ كبير، كالذي حدث عام 2013 في متاجر تارغيب، تهبط أسعار البطاقات المسروقة أكثر بعد نتيجة توفر عرضٍ أكبر بكثير من الطلب في السوق. وتباع البطاقات على مواقع الشبكة المظلمة مثل مازافاكا وتورتوغا وكاردر بلانيت وشادو كرو وأبروفن والاتحاد الدولي لتحسين النشاطات الإجرامية (إياسا)، وهو موقعي المفضل. تتطلب جميع هذه المواقع تقريباً التسجيل فيها، ويخضع الأعضاء للتمحيص بهدف تجنب دخول الشرطة، ويَعِدُ لصوص البطاقات بـ "نسب صلاحية عالية"، ويقدمون ضمانات بأن تعمل 95

بالمئة من بطاقاتهم الائتمانية المسروقة، وإلا "يمكنك استعادة مالك". أما الأرباح التي يحققها لصوص البطاقات العاملون في هذا المجال، فهي مترنحة بعد أن خسرت 11 مليار دولار سنوياً لمصلحة الاحتيال ببطاقة التسديد الشامل. والولايات المتحدة هي الضحية الكبرى لهذه السرقات حيث تعود إليها 47 بالمئة من جميع النشاطات الاحتيالية المتعلقة بالبطاقات.

انتحال الهوية

يسودُ الأوساط السريّة الرقميّة الاستخدام غير الشرعي لمعلومات التعريف الشخصيّة، وتتسرب مثل هذه المعلومات من سماسرة البيانات غير المحميين ومواقع الوسائط الاجتماعيّة، والتعامل غير السليم مع مناقلاتك الطبيّة والماليّة والتعلميّة والضريبيّة والتسوقيّة على الإنترنت. وتسمى هذه الهويات المسروقة غالباً بـ"الوبر" من قبل القراصنة، وهي تشتمل على الأسماء والعناوين وأرقام الضمان الاجتماعي وتواريخ الميلاد وأماكن العمل وأرقام الحسابات المصرفيّة، وأرقام التحويل المصرفي وأرقام رخص القيادة الصادرة عن الولاية، واسم عائلة الأم وعناوين البريد الإلكتروني وغيرها من أسماء الحسابات الإضافيّة على الإنترنت مع كلمات مرورها. وقد سبق لـ 20 بالمئة من المواطنين الأميركيين والأوروبيين أن وقعوا ضحية انتحال هوية. وتحقق مبيعات معلومات التعريف الشخصيّة في شبكة الويب المظلم أرباحاً هائلة، فسرقة الهوية الطبيّة (أي المطالبة بتعويضات باستخدام هويات مسروقة) تكبد نظام الرعاية الصحي 5.6 مليارات دولار سنوياً، بينما ستكلف سرقة الهوية بهدف التعويض الضريبي (أي أن يتقدم شخصٌ ما بطلب استرجاع ضرائب باسمك ليحتفظ بالنقود لنفسه) دائرة الإيرادات الداخلية 21 مليار دولار على مدى السنوات الخمس القادمة. كل هذا لأننا نسرب كمياتٍ ضخمة من البيانات من أنظمةٍ ضعيفة الأمن يمكن

الإتجار بها مقابل أرباحٍ هائلة في الشبكة المظلمة.

الوثائق

يمكن بسهولة شراء أي عددٍ من الوثائق على الإنترنت، بما فيها جوازات السفر ورخص القيادة وأوراق المواطنة والهويات المزوّرة والشهادات الجامعية وجداول العلامات وأوراق الهجرة، بل وحتى بطاقات الهوية الديبلوماسية. وتقوم شركات الشبكة المظلمة، مثل شركة أونيون لخدمات الهوية بكل سرور ببيع جوازات السفر وبطاقات الهوية بالبيتكوين. أما المستندات، فيتم استخدامها من قبل المجرمين والإرهابيين لتسهيل حركتهم بحرية عبد الحدود الدولية ولانتحال شخصياتٍ جديدة والقيام بغسيل الأموال. وكثيراً ما يتم إرسال رخص قيادة أميركية (من أية ولاية) بجودةٍ عالية جداً من الصين أو روسيا وبكلفة تقريبية تبلغ 200 دولار، بينما تُباع جوازات السفر التي تشحن من الولايات المتحدة أو المملكة المتحدة مقابل بضعة آلاف من الدولارات.

الأسلحة والذخيرة والمتفجرات

يتوفر أي سلاحٍ يخطر لك أن تشتريه تقريباً على الإنترنت عبر الويب المظلم على مواقع مظلمة، مثل أرموري وبلاك ماركيت ريلوديد وليبر.إيي.تور، التي يتم فيها بسهولة الإتجار بالمسدسات مثل مسدسات غلوك وبيريتا ومسدسات 9 مم الآلية. كما تتوفر البنادق الهجومية كالكلاشنيكوف والبوش ماستر (التي تستخدمها القوات الخاصة في أفغانستان والقادرة على إطلاق 700–950 رشقة في الدقيقة في النمط الآلي الكامل). ولا يتطلب الشراء فترات انتظار أو تحقيقات. كما تتوفر في هذه المتاجر متفجرات سي – 4 يقدمها مزودٌ ينوّه مسروراً إلى إمكانية "الشحن إلى جميع أنحاء العالم". ويمثل الشحن بالطبع مشكلةً إلى حدٍ ما، إذ لا يمكن

ببساطة إرسال رشاش أوزي مع شركة فيديكس دون أن تقرع أجراس الإنذار. وقد اعتاد موردو الأسلحة في الشبكة المظلمة هذا التحدي، فصاروا يرسلون منتجاتهم في طرودٍ مدرّعة يموّهونها بحيث تبدو وكأنها منتجاتٌ أخرى. حيث يتم تفكيك البنادق إلى قطعٍ أصغر وإرسالها بواسطة وسائل الشحن الخاصة. بل إن تجار الأسلحة يستطيعون ترتيب عمليات "إسقاط ميت"، يتم فيها إخفاء الأسلحة المجمعّة عبر دفنها في حديقة أو حاوية قمامة أو زقاقٍ، وبعد التسديد يتلقى الشاري إحداثيات الموقع الجغرافي وأوصاف السلعة المخفية. وحتى الأسلحة العسكرية تتوفر على الإنترنت هذه الأيام. فثمة مستخدمٌ في الويب المظلم يستخدم اسم بوهيكا، يعرض بشكلٍ أساسي أسلحة صغيرة للبيع لكنه ينوّه إلى أنّه "إذا كنت بحاجةٍ إلى مدفعية أو مان باد (أي نظم الدفاع الجوي المحمولة) أو معدات حربية أو ناقلة جنود مدرّعة، فالموارد متوفرةٌ لدينا ويمكننا توفير بعض الشروح مقابل رسوم. يرجى إرسال الرسالة القادمة مع تشفير بي.جي.بي. مفتاحنا العمومي هو صفحة الحساب هذه".

القتلة المأجورون

كما رأينا في طريق الحرير، يمكن تنظيم الاغتيالات بنقرةٍ واحدة في الشبكة المظلمة. ويسوّق مقدمو مثل هذه الخدمات، مثل Killer for Hire وQuick Kill وContract Killer وC'thulhu، جميعاً لـ "حلول دائمة للمشكلات الشائعة". وينوّه المرتزقة الذين يقدمون هذه الخدمات بفخرٍ إلى التدريبات العسكرية التي خضعوا لها، في الفيلق الفرنسي الخارجي على سبيل المثال، وإلى قدراتهم على القنص التي شحذوها في العراق وأفغانستان. ولكلٍ من هذه الخدمات قواعدها وتعليماتها الخاصة. فلدى إحداها سياسة "لا قاصرين" صارمة، فهي ترفض اغتيال الأطفال تحت سن الثامنة عشرة، بينما تحتّج خدمةٌ أخرى عندما

يتعلق الأمر بالاغتيال السياسي. لكن لا داعي للقلق، فثمة ما يكفي من مثل هذه الخدمات التي تسمح بالتكليف بقتل الشخصيات الحكومية، مثل موقع "سوق الاغتيال" الذي يعمل بالتمويل الجماهيري والذي ذكرناه سابقاً. وتتراوح الأسعار بين 20 ألف دولار وأكثر من مئة ألف دولار هي تكلفة قتل ضابط شرطة. وتطلب منك هذه المواقع تقديم صورةٍ حديثة للهدف إضافةً إلى عنوان العمل وعنوان المنزل والعادات اليومية والأماكن التي يتردد إليها. وتُستقبل الدفعات بالبيتكوين بكل سرور، كما يقدم دليلٌ على تنفيذ الجريمة بالصور كجزءٍ من الصفقة.

الإتجار بالبشر

يسهّل الويب المظلم عمليات الإتجار بالكائنات البشريّة أيضاً. وتختص كثيرٌ من مواقع الويب في بيع البالغين والقُصّر على حدٍ سواء والإتجار بهم. وتقدّر وزارة العدل الأميركية عوائد هذا الإتجار بـ 32 مليار دولار في السنة تذهب أرباحاً نقدية لشركة الجريمة. وبينما تبقى قنوات الإتجار التقليدية قائمةً، فإنّ التقانات الشبكيّة تمنح المتاجرين "قدرةً غير مسبوقة على استغلال عدد أكبر من الضحايا والتسويق لمنتجاتهم في ما يتجاوز الحدود الجغرافية". ففي الولايات المتحدة لوحدها يتم الإتجار بحوالى 200 ألف طفل من أجل الجنس، ويمكن لقوّادٍ أن يجني 150 ألف إلى 200 ألف دولار في السنة من كل طفل. وقد صرّح 70 بالمئة من الناجين من عمليات الإتجار بالأطفال بأنّه قد تم التسويق لهم على الشبكة في مرحلةٍ ما خلال رحلتهم مع الإتجار، وأنّهم كانوا يجبَرون على ممارسة الجنس بما يصل إلى عشرين مرّة في اليوم. وتتم ممارسة هذه النشاطات لا فقط على الويب المظلم بل وأيضاً على نحوٍ علني نسبياً على الويب السطحي وعلى الوسائط الاجتماعية من خلال إعلانات سريّة، فثمة مواقع ويب، مثل باك بيج، تروّج لـ "مرافقة" و"مساجّات". وتولّد إعلانات القوّادين حوالى 45 مليون دولار

في السنة تمثل عوائد لشركات سريّة على الإنترنت. وليس الأطفال هم الوحيدين الذين يباعون على الإنترنت، فالمهاجرون وأبناء الفئات المهدّدة يعرضون للبيع أيضاً.

الإتجار بالأعضاء البشريّة

توجد في جميع أنحاء العالم سوقٌ سوداء نشطة ومروّعة لأعضاء الجسد البشري. حيث يمكن جني 200 ألف دولار مقابل الكُلى، و120 ألف دولار مقابل القلوب، و150 ألف دولار مقابل الأكباد، وعشرة دولارات فقط لكل إنش مربع من الجلد، و500 دولار مقابل الكتف، و1500 دولار مقابل زوجين من العيون. فمن أين تأتي هذه الأجزاء البشرية؟ من الأموات كما من الأحياء. فنهب القبور ما يزال قائماً في القرن الحادي والعشرين، والكثير من مستودعات الجثث في أنحاء العالم تقوم ببيع أعضاء أولئك الذين عُهِد بهم إليها، مفترضةً عن حق بأنّ عائلاتهم لن تعرف بالأمر أبداً. والأسوأ من ذلك هو الخطر الكبير الذي يتهدد الفقراء الأحياء الذين يتم استهدافهم على الإنترنت وخارج الإنترنت بغزارة لبيع أعضائهم للمرضى الميسورين، الذين يكونون في حاجةٍ ماسّة إليها. ففي الولايات المتحدة لوحدها يوجد أكثر من مئة ألف شخص على قائمة الانتظار لتلقي الكُلى، ما يعني فترة انتظار تصل إلى عشر سنوات، لكن معظمهم يموتون خلال نصف هذه المدة. لذا فإن المرضى الميسورين يتوجهون إلى ما وراء البحار بحثاً عن "متبرعين"، محفّزين تجارةً محظورة مزدهرة بالأعضاء البشرية. ولدى شركة الجريمة قسمٌ كامل من سماسرة الأعضاء المتفرغين للإتجار بالأعضاء البشرية الذين يعملون كوسطاء يربطون بين القارات، ويصلون الباعة والشراة بعضهم ببعض ويرشدونهم إلى أطباء وجراحين ومرافق صحيّة متآمرة مع السماسرة. وتقدّر منظمة الصحّة العالميّة أن عضواً تم الحصول عليه بطريقةٍ غير شرعيّة يتم بيعه كل ساعة في شبكات الأوساط السريّة هذه.

وقد تأتي هذه الأعضاء من سجناء تم إعدامهم في الصين، أو من نساءٍ يجبرهن أزواجهن على بيع أعضاء أجسادهن بهدف المساهمة في دخل العائلة، أو من لاجئين سوريين وصلوا لتوهم إلى لبنان وهم في أمسّ الحاجة إلى السيولة النقديّة. ومع أن الكلية قد تباع مقابل 200 ألف دولار، فإنّ أولئك الذين تبرعوا يحصلون على مبلغٍ أقل من ذلك بكثير، ربما لا يتجاوز 250 إلى 10 آلاف دولار ما يترك هامش ربحٍ هائلاً لسماسرة الأعضاء المجرمين. والمحزن في الأمر هو أنّ أولئك الذين يبيعون أعضاء جسدهم لا يتلقون سوى قدرٍ ضئيل من رعاية ما بعد العمل الجراحي، هذا إذا تلقوا رعايةً أساساً. وكثيرون منهم يموتون على أثر العمليات الجراحية. تمارس هذه النشاطات على نحوٍ متزايد على الإنترنت وفي غرفة المحادثة وفي الويب المظلم. ويقوم المُعدَمون في أماكن مثل الهند وبلغاريا وصربيا بنشر توسلاتهم اليائسة، كهذا المنشور الذي وضعته ربة منزلٍ مُحَدِّدةً زمرة دمها ورقم هاتفها "أنا مستعدة لبيع كليتي أو كبدي أو أي شيء يلزم من أجل بقائي". وفي الصين يستهدف سماسرة الأعضاء على نحوٍ خاص الشباب في منتديات الإنترنت، مستخدمين عباراتٍ مثل "تبرع بكلية واشترِ آيباد جديداً". وثمة حادثةٌ واحدةٌ على الأقل اكتُشف فيها صبي في السابعة عشرة، وهو يعاني صحةً سيئة اليوم، بعد أن قَبِل الصفقة عندما اكتشفت أمه الآيباد الجديد في منزل العائلة المُعدمة واتصلت بالشرطة.

عملات الظلام

لعملة البيتكوين مشكلاتها، لكنها لا تدّعي الكمال.

دان كامنسكي، من مجلة ويريد

تمكّن التقانة أشكالاً جديدة من العملة. ويَعِدُ الاقتصاد الرقمي المتنامي بتأمين أدواتٍ مالية جديدة خصوصاً لفقراء العالم وأولئك الذين لا تتوافر لديهم خدماتٌ مصرفيّة. وغالباً ما تكون هذه العملات الافتراضيّة الجديدة

مُغفلة الهوية. ولم تنل أي منها الاهتمام الإعلامي الذي حظيت به عملة بيتكوين، وهي شكلٌ رقمي من المال يُدار بطريقة لا مركزية تعتمد على العلاقات الزوجية بين المشتركين. وقد تم اختراع البيتكوين من قبل شخصٍ غامض (أو مجموعةٍ من الأشخاص) عام 2009 كان يدعو نفسه ساتوشي ناكاموتو، وكانت الأموال تُخلق أو "تنقّب" عبر حلّ معادلاتٍ رياضية تزداد صعوبةً وتتطلب طاقةً حسابية عالية. والنظام مصممٌ بحيث لا يسمح بخلق أكثر من 21 مليون بيتكوين على الإطلاق، مانعاً بذلك قيام سلطةٍ مركزية بإغراق السوق بالعملات الجديدة. يشتري معظم الناس البيتكوين في بورصات يقدمها طرف ثالث مقابل عملات تقليدية كالدولار أو اليورو أو باستخدام البطاقات الائتمانية. وتتأرجح أسعار الصرف مقابل الدولار تأرجحاً كبيراً، إذ تراوحت من خمس سنتات للبيتكوين الواحد عند ظهور العملة وأكثر من 1240 دولاراً في تشرين الثاني عام 2013.

ويمكن للناس إرسال المبالغ بالبيتكوين بواسطة الحواسب والتطبيقات النقالة، حيث يتم تخزين الأموال في "محفظات رقميّة". ويمكن تبادل مبالغ البيتكوين مباشرةً بين المستخدمين في أي مكانٍ في العالم باستخدام معرّفات أبجدية - رقميّة مميزة أشبه بعناوين البريد الإلكتروني من دون رسوم للمعاملة. وحين تتم عملية شراء يتم تسجيلها في سجلٍ عام يُعرف باسم "سلسلة الوحدات"، يضمن عدم إجراء مناقلاتٍ مكرّرة. والبيتكوين هي العملة الأكثر تشفيراً في العالم، لأنها تعتمد على "التشفير للتحكم بخلق وتحويل الأموال بدلاً من الاعتماد على سلطاتٍ مركزية". وقبول البيتكوين يتنامى بسرعة، فمن الممكن استخدامها لشراء الحلوى في سان فراسنيسكو أو الكوكتيلات في مانهاتن أو الشطائر في مترو الأنفاق في آلن تاون. كما يمكن استخدامها لشراء سيارة تسلاإس جديدة أو لدفع فاتورة دايركت. تي في أو للتسجيل على موقع أوكيوبيايد أو حتى لحجز تذكرةٍ على رحلة

فيرجن غالاكتك الفضائية التي سيقدمها ريتشارد برانسون.

نظراً لإمكانية إنفاق البيتكوين على الإنترنت دون الحاجة إلى حسابٍ مصرفي أو هوية لشراء أو بيع العملة المشفّرة فإنها تمثل نظاماً مريحاً لإجراء المناقلات مع إغفال الهوية، أو للدقة باستخدام هويةٍ مستعارة، حيث يبقى اسم المستخدم الحقيقي مخفياً. ومع أن البيتكوين لا تختلف عن أشكال العملة الأخرى نظراً لإمكانية استخدامها لأهدافٍ قانونية أو محظورة، فإن تقنيات تشفيرها وإغفالها النسبي للهوية يجعلها أكثر جذباً بكثير للمجرمين. ونظراً لعدم تخزين أرصدتها في موقعٍ مركزي، فإنه لا يمكن للشرطة بسهولةٍ أن تصل إلى هذه الحسابات أو أن تجمّدها، كما أن تعقب المناقلات المسجّلة في سلسلة الوحدات أعقد بكثير من مجرد إصدار مذكرة استدعاء بحقّ مصرفٍ محلي يعمل بواسطة الشبكات المالية المضبوطة تقليدياً. لذلك فإن معظم التجارة المحظورة في شبكة الويب المظلم تتم باستخدام أنظمة عملة بديلة. فما من أحدٍ يرسل شيكاتٍ ورقيّة أو يستخدم بطاقات ائتمانية عليها اسمه لشراء المخدرات أو صور الاستغلال الجنسي للأطفال. بل يلجأ هؤلاء إلى الأشكال الافتراضيّة والرقميّة مغفلة الهوية للعملة مثل بيتكوين.

في أيام آل كابون في فترة حظر التهريب التي سادها الابتزاز، كانت تعويذة المسؤولين الفيدراليين هي "تتبع المال". وقد كانت تُهم التهرب الضريبي هي التي أوقعت في النهاية بأكبر زعماء الجريمة في العالم في ثلاثينيات القرن العشرين لا الإدانات الجنائية. ومع أنّ هذه التعويذة بقيت العقيدة الأساسية في تطبيق القانون منذ ذلك الحين، فإنه سيكون على رجال الشرطة قريباً أن يجدوا شعاراً جديداً. فثمة اليوم أكثر من 70 عملة افتراضية مشفرّة تنافس البيتكوين، مثل ريبل ولايتكوين ودوجكوين، ويُقدَر حجم التداول بالعملات الافتراضية عام 2013 وحده بعشرة مليارات

دولار. نظراً للمبالغ الكبيرة المتداولة، فلا عجب في أن المجرمين لا يكتفون بتداول البيتكوين بل يستهدفون هذه العملة المشفّرة بالسرقة أيضاً. وقد تمكن القراصنة بالفعل من سرقة الملايين والملايين من الدولارات على شكل عملة افتراضية من بعضهم البعض، وكان أكبر هجومٍ حتى اليوم قد استهدف إم تي.غوكس وهي سوق بيتكوين في طوكيو سُرق من حقائبها الرقميّة 470 مليون دولار في بداية عام 2014. ولا شك في أنّ هذا سيكون مستقبل السطو على البنك، أما شركة التأمين على الودائع الفيدرالية فلن تغطي خسائرك التي تتكبدها بالبيتكوين بالطبع.

بعيداً من العملات المشفّرة، ثمة العديد من أشكال التسديد الإلكتروني الأخرى التي تفضلها شركة الجريمة وتقدمها شركات مثل ليبرتي ريسيرف وإي.غولد وويبموني. وقد اتهمت شركةٌ واحدة من هذه الشركات هي ليبرتي ريسيرف بغسيل أكثر من 6 مليارات على مدى بضع سنوات وفقاً للمدعين الفيدراليين. فقد سهلت الشركة، المعروفة بـ باي بال المجرمين، "حيث لا يلزم وجود حسابٍ شخصي مفصل"، طيفاً واسعاً من نشاطات شركة الجريمة عبر الويب المظلم منها "الاحتيال بالبطاقة الائتمانية وانتحال الهوية والاحتيال الاستثماري وقرصنة الحاسب والموادّ الإباحية للأطفال والإتجار بالمخدرات". كما يعتقد أنها أدت دوراً مركزياً في الحملة التي استهدفت الصرافات الآليّة بواسطة التعهيد الجماهيري التي نوهنا لها سابقاً وانتهت بسرقة 45 مليون دولار خلال عشر ساعات عام 2013. وعلى الرغم من إسقاط الشركة، كما حصل مع طريق الحرير، في النهاية من قبل مكتب التحقيقات الفيدرالية والقبض على مؤسسيها، فإن العديد من منافسيها ظهروا فجأةً ليحلوا مكانها. وتمتاز هذه الأسواق الجديدة عادةً ببنية لا مركزية تعتمد على العلاقات الثنائية وتتميز بمجموعةٍ من العملات المشفّرة من الجيل الأحدث. وهي تَعِدُ لا فقط باستخدام هويات مستعارة كالتي

تُسجل مشاعاً على سلسلة وحدات بيتكوين، بل بإغفال الهوية كلياً مع غياب إمكانية التتبع. من بين هذه العملات الجديدة عملة داركوين (أو عملة الظلام) التي يمكن اعتبارها نسخةً من بيتكوين في غاية السريّة، تعيش في الظل تمّ تطويرها خصيصاً لتمويه مشتريات المستخدمين عبر دمج أية مناقلةٍ تتم بمناقلات المستخدمين الآخرين، بحيث لا يمكن الربط بين أية عملية تسديد وبين فردٍ بعينه. وتتمتع دارك كوين بشعبيةٍ تزداد بسرعة وقد تصاعدت قيمتها بسرعةٍ هائلة من 75 سنت للواحدة إلى حوالى 7 دولارات بعد إدخالها بفترةٍ قصيرة.

وثمة أداةٌ أخرى تدعى دارك واليت (أو محفظة الظلام)، طورتها منظمةٌ تسمي نفسها أنسيستيم، تطمح إلى إعادة البيتكوين إلى جذورها التحرريّة عبر تمكين المناقلات "فائقة الإغفال للهويّة". وتطمح عملة دارك واليت التي تعمل تحت شعار "ليحلّ الظلام" إلى "أن تكون تطبيق البيتكوين المفضل لدى الفوضويين"، بل إنّ مطوريها يصفونها بأنّها "برمجية لغسيل الأموال". فعبر دمج تسديدات المستخدمين وتشفيرها تسمح هذه العملة بـ "تدفقاتٍ مالية لا يمكن تعقبها عملياً" عبر الأوساط السريّة الرقميّة. أما المجرمون المسلحون بهذه الأدوات المالية الجديدة فهم مسرورون ومستعدون للذهاب إلى التسوق، وثمة الكثير ليشتروه.

الجريمة كخدمة

مع توفر نظام عملةٍ غير شرعيّة غير قابلة للتعقّب، لم تعد الجريمة شيئاً تقوم بارتكابه فقط بل باتت شيئاً يمكنك شراؤه. فالجريمة كخدمة (أو كاس) هي نموذج تجاري جديد يسمح بتكليف آخرين بتنفيذ هجومٍ كامل أو جزءٍ منه، بينما يضمن متعهد الجرائم الذي ينظم المشروع ويستثمر فيه الأرباح لنفسه. وتماماً كما يزداد اعتماد الشركات الكبيرة على البرمجيات كخدمة لتنفيذ عملياتها التجارية التي تتجاوز إمكاناتها الأساسية، كذلك

يفعل المجرمون.

ومن بين الخدمات الأكثر شراءً تلك المتعلقة بالبنية التحتية لتقانة المعلومات، التي تمثل الأساس التقني الذي لابد منه لتشغيل أية مؤسسةٍ حديثة ناجحة. لكن شركة الجريمة لديها احتياجاتها الخاصة في ما يتعلق بالبنية التقانية التحتية، خصوصاً حين يتعلق الأمر بالبضاعة التي أصبحت في غاية الندرة هذه الأيام: الخصوصية وإغفال الهويّة. فقد اجتاح المجرمون الويب المظلم لأنه يقدم لهم أفضل فرصةٍ لتجنب نماذج الرقابة التجارية التي يُروِج لها فايسبوك وغوغل والقدرات ذات مستوى الدولة التي كشف عنها إدوارد سنودن. ونظراً لكون قابلية استمرارهم، بل وحياتهم، تعتمد على ضمان إغفال هويتهم، يخصص أفراد شركة الجريمة موارد كبيرة للحفاظ على خصوصيتهم قبل أن يهاجموا أهدافهم أو يبيعوا بضائعهم المحظورة.

أما عملياً، فيعني ذلك أن اللاعبين غير الشرعيين في الأوساط السريّة الرقمية يستخدمون الشبكات الخاصة الافتراضية (في.بي.إن) على نحوٍ واسع، إضافةً إلى مخدمات وكيلة تُخفي عناوينهم على الإنترنت وتتكتم على مواقعهم. كما أنهم يعتمدون بكثافة على ما يسمى خدمات الاستضافة المضادة للرصاص، وهي شركات تقدم خدمات استضافة الويب في مناطق تشريعيّة مثل روسيا وأوكرانيا وتُرحِب بالمحتويات المحظورة ولا تحاول أبداً معرفة هويات زبائنها، وتقبل التسديد عبر ليبرتي ريسيرف وبعملة البيتكوين، وعادةً ما تتجاهل الطلبات مذكرات الإحضار التي تتلقاها من السلطة التنفيذية. ومن بين شركات خدمات كاس هذه شركة تدعى فريدويم هوستنغ (أو استضافة الحرية)، كانت أكبر خدمات استضافة الويب على شبكة تور، وقد اتُهِمت من قبل مكتب التحقيقات الفيدرالي بأنها أكبر مُسهِل لصور الاستغلال الجنسي للأطفال في العالم، حيث تدعم 95 بالمئة من المواد الإباحية الخاصة بالأطفال في العالم. وثمة المئات من

متعهدي الجرائم وموردي صور الاستغلال الجنسي للأطفال يدفعون المال لهذه الخدمة لقاء استضافتها لمواقعهم على الويب السري مع إغفال هوياتهم مع وجود آلاف المستخدمين المسجلين على كلٍ من هذه المواقع.

إضافةً إلى ما سبق، وتماماً كما لجأت الشركات بسرعة إلى الحوسبة السحابية لتخزين ملفاتها على خدماتٍ غوغل درايف وأمازون، كذلك فعلت شركة الجريمة. ففي تحولٍ لافتٍ للأحداث، لم يعد القراصنة يكتفون باستهداف بياناتك التي خزنتها على السحابة، بل بدأ يزداد انتفاعهم من مثل هذه الخدمات لسهولتها لتخزين ملفاتهم الأقل حساسية على الشبكة. فالسحابة مناسبةٌ على نحوٍ خاص للحاجات الحاسوبية لأفراد شركة الجريمة الذين يستخدمون البطاقات الائتمانية المسروقة، والهويات المزوّرة وشركات الواجهة لاستئجار المساحات لدى الشركات الشرعيّة بهدف استضافة برمجياتٍ خبيثة على مخدماتها. ومع استخدامهم لشركاتٍ لها سمعتها لاستضافة برمجياتهم الخبيثة، يصبح القراصنة أقل عرضةً لحجب عملياتهم أو لاكتشافهم من قبل طرفٍ ثالث. وهو توجهٌ يتصاعد، فقد بينت دراسةٌ عام 2013 أن 16 بالمئة من قنوات توزيع البرمجيات الخبيثة في العالم، كانت مُستضافةً على خدمة أمازون السحابية، بينما أتى 14 بالمئة منها من مُخدمات غودادي للاستضافة.

علاوةً على ما سبق، تضع السحابة قدراتٍ حسابيةً هائلة تحت تصرف المستخدمين الشرعيين والقراصنة على حدٍ سواء. لذا فإننا قد دخلنا عصر الحوسبة المسلّحة، الذي يمكن فيه لأي شخصٍ على الإطلاق يملك حفنة من الدولارات أن يصل إلى مستوياتٍ من الطاقة الحسابية لم يكن من الممكن تخيلها في السابق، سواءٌ استخدمها للخير أم الشر. فقد استخدم القراصنة الذي اقتحموا شبكة سوني بلايستيشن على سبيل المثال الطاقة الحسابية التي تقدمها خدمات أمازون للحوسبة السحابية لاختراق الآلاف من

حسابات المستخدمين وتفاصيل البطاقات الائتمانية. ويقلص "هذا الخلع السحابي" الوقت اللازم لكسر أعتى كلمات المرور، ليجعلنا جميعاً بذلك أقلّ أماناً. فباستخدام الطاقة الحسابية الموزعة للسحابة وأدواتٍ مثل كلاود كراكر يمكنك اليوم تجريب 300 مليون كلمة مرور في حوالى 20 دقيقة بتكلفةٍ تبلغ حوالى 17 دولاراً. أي إنّ أي شخصٍ بإمكانه استئجار خدمات الحوسبة السحابية لكسر مفتاح التشفير، الذي عادةً ما يحمي معظم شبكات وايفاي اللاسلكية في أقل من ست دقائق بتكلفةٍ زهيدة تبلغ 1.68 دولار كرسوم استئجار (لا شك في أنها ستنخفض أيضاً في المستقبل بفضل قانون مور).

تماماً كما يمكن للشركات الشرعيّة توظيف مبرمجي حاسب لمساعدتها على بناء مواقع الويب وكتابة البرمجيات، يمكن لشركة الجريمة أن تفعل ذلك أيضاً. وتصف شركة كرايم انفورسرز (والاسم هو تحوير لكلمة "السلطة التنفيذية") نفسها على سبيل المثال بأنّها "منظمةٌ خاصة مستعدة لتلبية احتياجاتك الخاصّة في مجال تطوير البرمحيات... إذا كانت بحاجة إلى عتادٍ معين... أو برمجيات لا يمكن تطويرها أو حتى مناقشتها في بلدك... فنحن نقدم خدمة تطويرٍ مغفلة الهوية وسريّة لتلبية احتياجات مشاريعك. ولا يهمنا ما الذي تُزمِع القيام به بالعتاد والبرمجيات التي تطلب منا إعدادها". لا أسئلة تطرح في عالم تطوير البرمجيات الإجرامية. ويمكنك تكليف شركات الجريمة الأخرى باقتحام أي نظامٍ تختاره، وستقوم بذلك ببراعة. فمن المعروف أن منظمة هيدن لينكس (أو الوشق المتخفي) الصينيّة، التي تضم ما يصل إلى مئة لص سايبري محترف، قد نجحت في اختراق نظمٍ تعود إلى غوغل وأدوب ولوكهيد مارتين وغيرها. ومن المخيف أن المنظمة تضم بين أفرادها ضباط جيش واستخبارات، يعملون لمصلحة الحكومة الصينية خلال النهار لتنفيذ عمليات سايبرية عدوانية بتكليفٍ من

الدولة. إلا أنّ كثيراً منهم بعد العمل يعملون على تحسين دخلهم تحسيناً كبيراً عبر العمل الإضافي، كمحتالين سايبريين وقراصنة بالتكليف. ويتميز هؤلاء عن القراصنة الاعتياديين بمهاراتهم المتقدمة. إنه عالم المرتزقة السايبريين الذي أصبح متوفراً كأي من عروض خدمات كاس الكثيرة الأخرى في الأوساط السريّة الرقميّة.

إضافةً إلى خدمات استئجار القراصنة، تُعَهّد شركة الجريمة طيفاً واسعاً من الخدمات الإدارية كالصيرفة والترجمة والسفر وعمليات مراكز الدعم الهاتفي.

فثمة خدماتٌ مثل CallService.biz على سبيل المثال تملأ فجوةً في الأوساط السريّة الرقميّة بتأمين خدمة كومبارس عند الطلب ناطق بالإنكليزية أو الفرنسية أو الألمانيّة، لمساعدة المحتالين على تجاوز الإجراءات الأمنيّة المصرفيّة الضرورية لتحويل الأموال، أو إعادة تفعيل الحسابات المخترقة أو تغيير معلومات العنوان عبر الاتصال بالمصرف. والمركز المتعدد اللغات الإجرامي الذي يعمل على مدار الساعة مستعدٌ لتأدية أي دور احتيالي ترغب به، بما في ذلك انتحال المرجعيات المهنية والتعليمية مقابل عشر دولارات للمكالمة الواحدة فقط. ويمكن لمتعهد الجرائم أن يجد أية خدمةٍ احترافية يحتاج إليها في العالم السري الرقمي. لكن هذه الخدمات تتحول باطّراد إلى سلعٍ يتم تجميعها وتغليفها وبيعها على شكل برمجيات إجرامية متوفرة على نطاق واسع في أعماق الويب المظلم.

جريمازون دوت كوم

اقتصاد الأوساط السريّة الرقميّة هو اقتصادٌ معقد، إذ لا يبيع المجرمون مباشرةً إلى المستهلكين (مخدرات ورخص قيادة مزورّة ومحتويات مقرصنة وغيرها) وحسب، بل يبيعون بالجملة مباشرةً بين بعضهم البعض. وبينما

يتمثل نموذج "الجريمة كخدمة" بشكلٍ أساسي في تأمين البنية التحتية الداعمة وإمكانات إغفال الهوية التي يتطلبها الحفاظ على دوران آلة الجريمة، فإن اقتصاد الأوساط السريّة حصل على الدعم مع بدء أفراد شركة الجريمة بتقديم أدواتٍ جاهزة للتصّيد وإرسال البريد المزعج والاحتيال وتنفيذ هجمات حجب الخدمة وسرقة البيانات.

فقد أدرك المبرمجون الإجراميون المتميزون أن أدوات الهجوم التي طوروها بأنفسهم قد تحقق أرباحاً إضافية إذا ما بيعت لزملائهم المجرمين، الذين يعوزهم الوقت أو الخبرة، لشن هجماتهم الخاصة. نتيجةً لذلك صار بإمكان المجرمين الأقل مهارةً أن يشتروا ببساطة الأدوات التي يحتاجون إليها عند الطلب لتحديد نقاط ضعف النظام الهدف أو انتحال الهوية أو اختراق المخدمات أو سرقة البيانات، إنها الجريمة بنقرةٍ من الفأرة.

وهكذا تحول الويب المظلم إلى "جريمازون" افتراضي، أكبر سوق على الإنترنت في العالم يذهب المجرمون للتسوق فيها. وفي هذه السوق يجدون أمامهم بازاراً تركياً يعجّ بالفاكهة المُحرمة مرتبةً على نحوٍ أنيق في انتظار مشتريها. وعلى غرار الموردين الآخرين في التجارة الإلكترونية، قامت شركة الجريمة بتطوير واجهات متاجر لمنتجاتها في الشبكة المظلمة، وزودت متاجرها بعربات التسوق ونظم التسديد ورموز للكوبونات ونظم معالجة عمليات التسديد والدعم الفني، وخدمة الزبائن عبر المحادثة المباشرة وخدمات الودائع. ويقدم الباعة خدمة التسوق من موقفٍ واحد، كما يمكنك ترك بطاقة أميركان إكسبريس الائتمانية في المنزل، فالباعة هنا يقبلون البيتكوين بكل سرور.

كمثال على ذلك، كانت البرمجية الخبيثة المسؤولة عن الاجتياح الواسع لنظام نقاط البيع لدى متاجر تارغيب في نهاية عام 2013 عبارة عن مجموعة أدوات برمجية إجرامية تُعرف باسم بلاك بوس. نستعرض في ما

يلي بعض الأدوات الإجرامية الأكثر شعبيةً المعروضة للبيع في الأوساط السريّة الرقميّة:

زيوس بيلدر: يتراوح سعرها بين 5000 و7000 دولار، وتقدم العديد من الوظائف التي تتراوح بين التسجيل السري لنقرات مفاتيح المستخدم وسرقة التراخيص الرقميّة المشفرّة التي تتطلبها الصيرفة على الإنترنت. وعلى مدى السنوات، وفقاً لتقديرات مايركوسوفت، أصيب بحصان زيوس الطروادي هذا أكثر من 13 مليون حاسب في أنحاء العالم وقد استخدم لسرقة أكثر من مئة مليون دولار.

باغات: تتخصص هذه الأداة، التي لا يتجاوز سعرها الألف دولار، في تقليد الحسابات المصرفية لإنجاز عمليات التحويل المالي. وقد استخدمت هذه الأداة عام 2010 في رسالة التصّيد الإلكتروني التي أرسلت إلى عشرات الملايين من مستخدمي لينكدإن، طالبةً منهم "تحديث حساباتكم". وعندما يفعلون، كان حصان طروادة يقوم بتنصيب برمجياتٍ خبيثة في متصفحات الويب لديهم خلال أقل من أربع ثوانٍ لتقبع بعد ذلك بصمت منتظرةً الفرصة لسرقة التفاصيل المالية، حين يتم تسجيل الدخول إلى الحسابات المصرفية في المرة القادمة.

سباي.آي: مقابل 500 دولار فقط، يقدم سباي.آي جميع ميزات زيوس وأكثر. وقد أشعل ظهوره في نهاية عام 2009 حرب أسعارٍ بين البرمجيات الإجرامية ونمت حصته في السوق نمواً سريعاً. وفي تحولٍ مدهش لحرب العصابات الشبكيّة، ضمّن مخترعو سباي.آي ما يشبه وحدة مكافحة

الفيروسات في برمجيتهم لاكتشاف وجود حصان زيوس الطروادي المنافس على آلات المستخدمين المصابة العامة. وحين يعثر عليه يقوم سباي.آي بسرور بإزالة زيوس المنافس وإصلاح نقطة الدخول، لضمان أن يكون هو البرمجية الخبيثة الوحيدة التي تعمل على الآلة الهدف. وعلى غرار منافسه زيوس، يُعتقد أن سباي.آي قد درّ مئات الملايين من الدولارات على مهندسيه.

تخضع الأدوات البرمجية التي تباع على جريمازون لتطويرٍ مستمر وتدأب شركات الجريمة على بيع تحديثات "الإصدارات الأخيرة" لضمان اشتمال برامجها على أحدث أنواع الهجمات الحاسوبية. وثمة بالطبع جريمازون الممتاز، وهو برنامجٌ يمنح العصابات الزميلة فرصة "الاشتراك والادخار" على مشترياتهم. ومن الأمثلة على هذه العروض أدوات بلاك شيدس المتوفرة للاستئجار الدائم، والتي تقدم للمستخدمين تحديثات مجانية غير محدودة ودعماً فنياً. وتجمع هذه الأداة، التي ربما كانت أكثر معدات هجوم بالبرمجيات خبيثة شهرةً وشعبية في العالم، بين الخفّة التقنيّة المدهشة ونموذج الأعمال المتقدم جداً، لدرجة أنه يبدو وكأنه قادم من دراسةٍ أعدّت في مدرسة الأعمال في هارفارد.

يمكن لمتعهدي الجرائم الذين ابتاعوا أدوات بلاك شيدس اختيار الطريقة التي تقوم بها البرمجية الخبيثة بمهاجمة الآلة المستهدفة، كتضمين حصان طروادة في ملف أو إخفائه في موقع ويب أو وضعه على قرص يو.إس.بي خارجي ينفث حمولته القاتلة حالما يُدخل في الحاسب الهدف. وتمنح برمجية بلاك شيدس، نظراً لكونها حصان طروادة متقدماً يمكن التحكم به عن بعد (رات)، المطورين تحكماً كاملاً وشاملاً على وظائف الآلة المصابة. لذلك كانت البرمجية قادرةً على تسجيل مدخلات لوحة المفاتيح وسرقة

كلمات المرور وشن هجمات حجب الخدمة، وخطف حسابات الفايسبوك وتنصيب برمجيات خبيثة إضافية على النظام المصاب. والأسوأ من ذلك أنها أصبحت الأداة المفضلة للمطاردين المبتدئين لأنها تسمح لسيدها بتشغيل ميكروفون أو كاميرا أي حاسب عن بعد لالتقاط أي صوت أو فيديو في محيطه البصري، من دون إعطاء أية إشارة مثل ضوء التسجيل الأخضر الصغير. وكانت البرمجية جيدةً إلى حدّ أن نظام بشار الأسد السوري استخدمها للتجسس على نشطاء الديمقراطية ضمن البلاد. وعلى الرغم من توفر أدوات الجريمة والتجسس التي تعمل بنقرة فأرة على نطاقٍ واسع في جريمازون، فإنّ أي هجوم حاسوبي يبدأ بالاختراق الأولي للنظام وبالعدوى بالبرمجيات الخبيثة، وهي نقاط ضعف متوفرة للبيع على نطاقٍ واسع في العالم السري الرقمي.

المجمع الصناعي للبرمجيات الخبيثة

> فقد علماء الذرّة براءتهم عندما استخدمنا القنبلة الذريّة للمرة الأولى. ويمكننا القول إنّ علماء الحاسب قد فقدوا براءتهم عام 2009 عندما بدأنا باستخدام البرمجيات الخبيثة كسلاحٍ هجومي.
>
> بيكو هيبونن

لكي يتمكن المجرمون والجواسيس والعسكريون والإرهابيون من تنفيذ هجماتهم السايبرية العدوانية، لا بد لهم أولاً من إيجاد طريقةٍ لاختراق نظام المعلومات المستهدف من قبلهم. وكما رأينا في هجوم دودة ستاكس نت ضد موقع التخصيب النووي الإيراني في ناتانز، قد يتطلب التخطيط لمثل هذه العمليات سنواتٍ من العمل ويكلف ملايين الدولارات. لكن من حسن حظ أولئك الذين لا يتوفر لديهم الوقت أو المال لتطوير أسلحتهم السايبرية الخاصة، ثمة سوق سوداء مخفية وواسعة يمكن للجواسيس والجنود واللصوص والناشطين – القراصنة أن يتسوقوا فيها، لشراء ما يدعى

هجومات اليوم صفر. فكما ذكرنا من قبل، لم يتم اكتشاف ثغرات اليوم صفر من قبل شركات البرمجيات ونظم مكافحة الفيروسات بعد. لذا فإنها تستطيع بسهولة تجاوز الإجراءات الأمنية والجدران النارية الشائعة من دون أن ينطلق جرس الإنذار.

اعتاد القراصنة في الماضي الاحتفاظ بمثل هذه الثغرات لاستخدامهم الشخصي، أو كانوا يحاولون بيعها إلى عمالقة البرمجيات مثل مايكروسوفت وياهو وغوغل، عبر برامج "المكافأة على التبليغ عن الثغرات" التي تقدمها هذه الشركات. لكن المكافآت في هذه البرامج كانت تافهة تُقدم 500 دولار فقط مقابل الكشف عن ثغراتٍ أمنية كبرى. ونتيجة لليأس، أدرك القراصنة أنه ثمة خياراتٌ أفضل بكثير متاحةٌ لهم، بما فيها بيع هذه الثغرات الأمنية في السوق المفتوحة للمجرمين والحكومات. وقاد هذا الإدراك إلى تأسيس شبكةٍ معقدة جداً من الشُراة والباعة والسماسرة الذين يتداولون الثغرات السايبرية في ما بات يعرف بـ "المجمع الصناعي للبرمجيات الخبيثة".

قبل أن تتمكن شركة الجريمة من بيع أدواتها الإجرامية السايبرية مثل سباي.آي وزيوس، عليها تجميع كمية من نقاط الضعف، التي يمكن استغلالها وتوضيبها في برمجياتٍ إجرامية يمكن لعامة المجرمين استخدامها. وهي تقوم بذلك عبر تمويل حملات شراء نقاط الضعف، وهي تمتلك الميزانيات المطلوبة لفعل ذلك. إذ تشير التقارير إلى أنّ قرصاناً إجرامياً يدعى باونش، قد كلفّ تاجر ثغرات وسيطاً وزوده بميزانيةٍ بلغت 100 ألف دولار لجمع نقاط الضعف، لكي يستخدمها في أداة الهجوم الخبيثة التي كان يطورها باسم بلاك هول (أو الثقب الأسود). لكن قرصاناً آخر يستخدم الاسم المستعار جي.بي.مورغان، وكأنّه لا يريد لأحدٍ أن يَبُزّه، نشر رسالةً في منتدى دارك كود الإجرامي معلناً فيها أن لديه ميزانيةً تبلغ 450 ألف دولار ستنفق لشراء ثغرات يمكن استخدامها في هجمات اليوم صفر، لكي يشملها

في الأداة البرمجيّة الإجرامية الاحتكاريّة الخاصة به. بل إنّ غرف محادثة الشبكة المظلمة تعجّ بطلبات شراء البرمجيات الخبيثة، ومن الشائع مشاهدة منشوراتٍ من قبيل "هل لديك أية ثغرة في ويندوز 7 تسمح بتنفيذ الشيفرة البرمجية؟ إذا كانت لديك فلا مشكلة في الدفع".

لا يقتصر الإتجار بالأسلحة السايبرية على المجرمين، فقد أصبحت الأجهزة الأمنيّة الحكومية زبائن تتردد على شراء مثل هذه الأدوات، حيث تلجأ إلى سماسرةٍ آخرين للحصول على ترسانتها التقنيّة. وقد فرض وسيطٌ اسمه غروك نفسه، ليصبح السمسار المفضل للثغرات الأمنيّة لقدرته على التفاوض على صفقاتٍ كبيرة بين أولئك الذين يكشفون عن الثغرات الأمنيّة وأولئك الذين يبحثون عنها ليقوموا باستغلالها. ففي عام 2012، باع غروك ثغرةً في نظام تشغيل آي.أو.إس للهاتف النقال لمتعاقدٍ مع الحكومة الأميركية، مقابل مبلغ لا بأس به بلغ 250 ألف دولار (تُقتطع منه عمولته المعروفة والبالغة 15 بالمئة).

ظهر عدد من الشركات الاحترافية، التي لا يحتوي نموذجها التجاري سوى على بيع الثغرات الأمنيّة الحاسوبية التي يمكن استغلالها بواسطة البرمجيات الخبيثة إلى الحكومات. فثمة شركات مثل فوبين في فرنسا ونيتراغارد في ماساتشوستش وإكسودس إنتلجنس في تكساس وريفونن في مالطا وإندغيم في جورجيا، جميعها تعمل على بيع الثغرات الأمنيّة لزبائنها في أنحاء العالم. وبينما تدقق بعض الشركات التي تبيع ثغرات يمكن استغلالها في شنّ هجمات اليوم صفر في هويات زبائنها، تبيع شركاتٌ أخرى لأي كان، من شركات الجريمة إلى الدكتاتوريات السيئة السمعة، من دون طرح أية أسئلة. والنتيجة، كما ينوه الباحث المعروف في مجال الأمن توم كيلرمان، هي أنه بإمكان أي شخص اليوم أن يُحمّل كلاشنيكوف سايبرية أو قنبلة يدوية سايبرية من مجموعةٍ كبيرة من المواقع.

تسمح هجمات اليوم صفر بشنّ هجماتٍ معقدة شديدة التخفي ضد أهدافٍ معينة، وقد أدت إلى ظهور ما درج باحثو الأمن على تسميته "التهديد المتقدم المستمر"، أو أي،بي،تي اختصاراً. وتجمع هذه الهجمات بين أبحاث الاستهداف الموسّعة ودرجةٍ عالية من التخفي، لإحكام سيطرتها على النظام الهدف لشهورٍ أو حتى سنواتٍ، وهي تشهد استخداماً متنامياً. ويقوم البرنامج العملياتي لهذه الهجمات السايبرية على الاختفاء والمراقبة والانتظار، أما القراصنة البارعون فيمحون دائماً سجلات النشاطات في النظام، بحيث لن تعلم أبداً أنهم كانوا هناك. وسواءٌ تم تطويرها من قبل الحكومة الأميركية أو الصين أم شركة الجريمة، فإنّ احتمال اكتشاف هذه التهديدات المتقدمة الدائمة بواسطة برمجيات مكافحة الفيروسات المعّدة للمستخدم العادي يكاد يكون معدوماً.

ربما تكون دودة ستاكس.نِت أشهر هذه البرمجيات الخبيثة، لكنّ لها أشباهاً مثل فليم ودوكو، إضافةً إلى الكثير مما لم نكتشفه بعد. والأسوأ من ذلك هو أنّ هذه الدودة، وهي أداة تم تطويرها لمهاجمة نظم التحكم الصناعي ولتعطيل شبكات الطاقة، خرجت عن السيطرة الآن وأصبحت متاحةً للتحميل، وقد تمت دراستها بالتفصيل من قبل شركة الجريمة، التي سرعان ما بدأت بمحاكاة تقنيتها وشيفرتها الحاسوبية لبناء أدوات هجومية أكثر تعقيداً بكثير. أما التحدي العميق الذي يواجهه مجتمعنا مع نمو المجمع الصناعي للبرمجيات الخبيثة، فيتمثل في أن هذه الأدوات الهجوميّة ما إن تستخدم مرةً واحدة حتى تتسرب وتصبح مشاعاً. والنتيجة هي انتشار الأسلحة السايبرية المفتوحة المصدر على نطاقٍ واسع وتوفرها في الأوساط السريّة الرقميّة، بحيث يمكن لأي شخصٍ إعادة تصميمها أو التسلح بها كما يرتأي. فكم سيمر من الوقت قبل أن يقوم أحدهم بالتقاط هذا المولوتوف الرقمي ليعيد قذفه علينا عبر مهاجمة نظم البنية التحتية

الحساسة لدينا؟ الخبر السيئ هو أن التحضيرات ربما كانت تجري اليوم بالفعل.

شبكة الأموات الأحياء: عندما تهجم زومبيات الشبكة الروبوتية

ليست نهاية العالم على يد الزومبيات التصور الأكثر إبهاجاً.

داناي غوريرا (ميشون) في الحي الذي يسير

من أكثر الأدوات فعاليةً في ترسانة القرصان الشبكة الروبوتية، أو البوتنيت، وهي شبكة من الحواسب المصابة التي تعمل تحت تحكم القرصان عن بعد. تتم السيطرة على هذه الآلات، التي تدعى الآلات الزومبية المصابة، وتُستَعبد موحدةً في شبكاتٍ روبوتية يمكن استغلالها في مجموعةٍ من الخدمات الإجرامية، مثل نشر البرمجيات الخبيثة والمشاركة في هجمات حجب الخدمة وتوزيع البريد المزعج أو في استضافة المحتويات المحظورة. ومن الممكن تجنيد الحواسب أو حتى الهواتف النقالة، في جيش من الشبكات الروبوتية عبر إصابتها ببرمجياتٍ خبيثة، وخصوصاً منها تلك التي تقدمها أدوات تطوير البرمجيات الإجرامية الجاهزة مثل بلاك شيدس وسباي.آي، المتوفرة على نطاقٍ واسع في الأوساط الرقميّة السريّة.

تعاني ضحايا مثل هذه الأدوات أثراً مضاعفاً لسوء الحظ، فهي لن تكتفي بسرقة تفاصيل بطاقتك الائتمانية وتاريخ عملياتك المصرفية وهويتك، بل ستترك في نظامك خلفها أيضاً باباً خلفياً يعطي شركة الجريمة مدخلاً دائماً إلى آلتك لتفعل بها ما يحلو لها.

فبينما تجلس أمام حاسبك تكتب ملفاً أو تقرأ أخبار سي.إن.إن على الإنترنت، ربما كان سيد الشبكة الروبوتية يستخدم آلتك في عددٍ من الخدمات الإجرامية. هل سبق لك أن تساءلت لماذا يعمل حاسبك بهذا البطء؟ ربما كنت تشارك من دون علمك في هجوم سايبري يجري شنّه ضد آخرين دون أن تكون لديك أية فكرةٍ عن حدوثة. فالشكر لك أنت على

خدمتك هذه.

يستخدم القراصنة التعهيد الجماهيري بتحويل هجومهم إليك وإلى حواسبك، ما يورطك من دون علمٍ في مؤامرتهم الإجرامية الدولية أنت وحواسبك. بل إنّ بوسع شركة الجريمة توريط حاسبك في شبكة زوجية للمحتويات الإباحيّة للأطفال، بأن تخفي صور استغلالٍ جنسي على سواقتك. فما الذي يدعوها في النهاية إلى المجازفة بالاحتفاظ بهذا المحتوى على شبكتها؟ نتيجةً للضعف الأمني لشبكتك ولعدم قدرتك على حماية أجهزتك الرقميّة، بتّ أنت أيضاً تشارك في اقتصاد الجريمة السايبرية. فكما يستفيد الفايسبوك من حياتك ومن حياتك الشبكيّة مالياً، كذلك تفعل شركة الجريمة.

من بين أشهر الشبكات الروبوتية شبكة ماريبوزا وكونفيكر وكوبفيس، مع وجود قادمين جدد مثل غيمأوفر زيوس يزيدون بسرعةٍ من حصتهم في السوق. فوفقاً لمكتب التحقيقات الفيدرالي، تسيطر شبكة غيمأوفر زيوس لوحدها على أكثر من مليون حاسب في أنحاء العالم، وقد تسببت بخسائر ماليّة بلغت 100 مليون دولار. وفي وسط عام 2014 كانت أكبر شبكة روبوتية معروفة في الوجود تدعى زيرو أكسيس، لا يقل عدد الحواسب الزومبية التي تحكم سيطرتها عليها عن المليونين. ومع تعاظم حجوم هذه الشبكات الروبوتية، تزداد قوتها الهجوميّة، حيث يمكن تدريب هذه الملايين من الحواسب على استهداف هدفٍ معين يتمّ اختياره لشنّ هجمة حجب خدمة. وتعمل هجمات حجب الخدمة عبر إغراق نظام حاسوبي أو موقع ويب بعشرات الآلاف من الطلبات الكاذبة، بما يؤدي في النهاية إلى انهيار الموقع الهدف ليخرج عن الشبكة أو يعجز عن إرسال البريد الإلكتروني أو تخديم صفحات الويب أو معالجة الطلبات أو إنجاز المناقلات المصرفيّة.

كما جميع أدوات وخدمات شركة الجريمة، يمكن شراء الشبكات الروبوتية الزومبية هذه أو استئجارها عبر الشبكة، ما يجعل هذه الأداة الهجوميّة الفعالة متوفرةً بتكلفةٍ زهيدة. ففي الأوساط الرقميّة السريّة الروسية يمكن شراء الشبكات الروبوتية القادرة على شنّ هجمات حجب خدمة فعالة مقابل 700 دولار، أو استئجارها مقابل دولارين للساعة فقط. وهي مدةٌ طويلة بما فيه الكفاية للتسبب بانهيار موقع ويب متوسط أو مركز دعم هاتفي. ويتمّ شنّ ما معدله ثلاثة آلاف هجوم من هذا النوع في أنحاء العالم كل يوم. علاوةً على ذلك، يزداد تعقيد هذا التهديد باستمرار مع لجوء كلٍ من شركة الجريمة والفاعلين الحكوميين، مثل إيران أو الصين، على نحوٍ متزايد إلى طاقة الحواسب الموزّعة الكبيرة على السحابة لتنفيذ هجمات حجب الخدمة. وثمة شبكة زومبيات معروفة باسم ستورم، كانت متوفرة للبيع في الأوساط السريّة الرقميّة في منتصف عام 2014 مقابل ثلاثة آلاف دولار فقط، تسيطر على 15 مخدماً سحابياً في أنحاء العالم وقادرةٌ على توليد بياناتٍ هجومية بحجمٍ يصعب تخيله يبلغ 300 غيغابايت في الثانية. وكان يجري التسويق لها على أنها أكثر من كافية لـ "إخراج بلدٍ صغير من الشبكة كلياً". تمثلت نتيجة وجود هذه الشبكات الروبوتية الزومبية في تسليح العالم السايبري من قبل شركة الجريمة.

تتزايد أعداد ضحايا هذا النوع من الاغتصاب السايبري بالشبكات الروبوتية. بل إنّ شركات مرموقة، مثل إيفرنوت وميت.آب، قد وقعت ضحية هذه الهجمات. وتنعَمُ شركة الجريمة بفضل هذه الترسانة من أدوات البرمجيات الخبيثة إضافةً إلى الملايين من زومبيات الشبكات الروبوتية في أنحاء العالم، بوسائل فعالة للسيطرة يمكن استخدامها كأسلحةٍ هجوميّة أو كآلات لدرّ الأموال أو لكليهما. نتيجةً لذلك دخلنا العصر الصناعي للجريمة الذي تخرج فيه شيفرات الحاسب الخبيثة من خط التجميع وكأنها منتجاتٌ

يتم تطويرها وبرمجتها خصيصاً بحيث تعمل بشكلٍ مستقل وتشن عدوانها ليل نهار، بينما يجني القراصنة أرباحهم المُجزية وهم نائمون.

ارتكاب الجريمة بقدرة آلة

على الرغم من الجهود التي تبذلها شركة الجريمة في التحسين المستمر للعملية التجارية لديها، فإنها لا ترتكب الجرائم الجديدة من الصفر كل مرة. ففي عصر قانون مور أصبحت هذه المهام مؤتمتةً إلى حدٍّ بعيد، ويمكن تشغيلها في الخلفية على نطاقٍ واسع دون الحاجة إلى تدخل بشري كبير. وتسمح أتمتة الجريمة لعصابات الجريمة المنظمة الدولية بتحقيق المستوى نفسه من الفعالية وادخار التكاليف الذي تحققه الشركات المتعددة الجنسيات، من خلال الاستفادة من التقانة في تنفيذ وظائفها التجارية الأساسية. وهو ما يسمح للقراصنة اليوم بنشل ليس شخصاً واحداً فقط بل مئة مليون أو أكثر كما رأينا في الاختراقات التي استهدفت سوني بلايستاشن وتارغيت.

تمارس أدوات الاختراق، مثل بلاك هول وسباي.آي، الجريمة "بقدرة آلة"، عبر أصغرة الحاجة إلى العمل البشري مخفضةً بذلك تكاليف الجريمة خفضاً هائلاً. كما أنها تسمح للقراصنة بالاستفادة من فرصة "الأثر الطويل" عبر ارتكاب ملايين السرقات لمبالغ صغيرة لا تُبلّغ عنها الضحايا ولا تستطيع السلطة التنفيذيّة تتبعها، بينما يتم استهداف أهداف معينّة ذات قيمة عالية (كالشركات والدول والمشاهير والأغنياء أو الأشياء المرغوبة أو تلك التي يراد التخلص منها) بخططٍ تُعدّ خصيصاً لها. وتُخترق غالبية الأهداف العامة بواسطة برمجيات حاسوبية خبيثة مؤتمتة تعمل في شبكة تصيّد رقميّة ضخمة، تستهدف كل شيء وأي شيء على الشبكة باستغلال ثغرةٍ أمنيّة معينة. ونظراً لهذه المنافع الواضحة، شُنّ 61 بالمئة من مجمل الهجومات على الإنترنت عام 2011، كما تشير التقديرات، بواسطة أدوات

جريمة مؤتمتة بالكامل عادت بأرباحٍ فلكية على لوردات الويب المظلم، الذين كانوا يستخدمون خبراتهم في تنسيق هذه الهجمات. لقد تمّ اختصار الجريمة الحديثة وتقطيرها لتتحول إلى برنامجٍ حاسوبي يستطيع أي شخصٍ تشغيله لتحقيق أرباحٍ هائلة.

يمكن استخدام الشبكات الروبوتية وغيرها من الأدوات لا فقط لشن هجوم أو ارتكاب جُنحةٍ ما مراراً وتكراراً، بل هي تمكّن من ارتكاب جرائم أعقد بكثير، مثل الابتزاز أو الانتزاع أو التفتيش. ففي نسخةٍ محدّثة من البريد المفخخ الذي كانت ترسله شركة إينوفتف ماركتنغ الأوكرانية ليعود عليها بـ 500 مليون دولار والذي كان يبلّغ المستخدمين بـ "اكتشاف فيروس"، أصدرت شركة الجريمة ملف تورنت جديد للبرمجية الخبيثة يستطيع أخذ حاسبك رهينة، إلى أن تدفع فديةً لتتمكن من الوصول إلى ملفاتك من جديد. وتتوفر أدوات الهجوم هذه، المعروفة ببرمجيات الفدية، في مجموعةٍ واسعة من أدوات الشبكة المظلمة مثل غيمأوفر زيوس. وثمة العديد من التنويعات على هذه الرسالة منها واحدةٌ تدّعي أنها قادمةٌ من السلطة التنفيذية. فقد فوجئ المستخدمون الذين أصيبوا بحصان ريفيتون الطروادي في أنحاء العالم بحواسبهم تُقفل، وقد غطت شاشاتها ملاحظةٌ تدعي أنها من مكتب التحقيقات الفيدرالي. وكانت الرسالة، التي تحمل رمزاً كبيراً ملوناً لمكتب التحقيقات الفيدرالي يبدو رسمياً، تدعي بأنّ حاسب المستخدم تم إقفاله لأسبابٍ مثل "خرق قانون الملكية الفكرية الفيدرالي عبر تحميل مواد غير مشروعة من الإنترنت" أو لأنك "كنت تستعرض أو توزع محتوى إباحياً محظوراً".

ولفكّ قفل حواسبهم، بُلّغ المستخدمون بأنّ عليهم دفع غرامةٍ تتراوح بين 2 و400 دولار لا تُقبل سوى باستخدام قسيمةٍ مسبوقة الدفع من نوع موني باك من غرين دوت، أُعلم الضحايا بأنّه بإمكانهم شراؤها من متجر وول

مارت محلي أو سي.في.إس. وللإمعان في إذلال الضحايا وفي إقناعهم بأنّ الموضوع أصبح قضيةً جادة لدى الشرطة، تعرض شركة الجريمة على نحوٍ بارز عنوان الإنترنت للضحايا التي يُزعم أنها اخترقت القانون، إضافةً إلى مقاطع فيديو تكون قد التقطت قبل ذلك بواسطة كاميرا الويب. وقد نجحت الرسالة في استهداف عشرات الآلاف من الضحايا في أنحاء العالم مع تعديلها محلياً وفقاً للبلد واللغة ووكالة الشرطة. فكان المستخدمون في المملكة المتحدة يستقبلون المُذكرة من اسكوتلانديارد ويتلقاها الأوروبيون على شكل تحذيرٍ من الأويروبول، بينما يرى الضحايا في الإمارات العربية المتحدة التهديد مترجماً إلى العربية، مُدعياً أنه صادر من رئاسة شرطة أبو ظبي.

ظهر نوعٌ آخر من الابتزاز المؤتمت أكثر خبثاً بعد مثله كريبتولوكر، وهو حصان طروادة يقوم بتشفير جميع الملفات على حاسب الضحية، بحيث لا يعود بإمكانها قراءة هذه الملفات أو الوصول إليها. ثم تعرض البرمجية الخبيثة على نحوٍ مرعب ساعة عدٍ عكسي أشبه بساعة القنبلة الموقوتة، تُخبر المستخدمين بأنّ لديهم 48 ساعة فقط لدفع مبلغ 300 دولار وإلا فإنّه سيتم تدمير جميع ملفاتهم نهائياً. وتقبل هذه البرامج، التي تبدو وكأنها تقول "إذا أردت أن ترى ملفاتك قيد الحياة مرةً أخرى"، الأموال بالبيتكوين بكل سرور. ولم تكن الرسالة التي توجهها برمجيات الابتزاز هذه لضحاياها مجرد تهديدٍ فارغ. فبينما كانت برمجيات الابتزاز في السابق تخدع المستخدمين عبر إخفاء ملفاتهم مؤقتاً، فإنّ كريبتولوكر كان يستخدم في الحقيقة تشفيراً قوياً وفق معيار التشفير المتقدم، الذي يستخدم 256 بتاً لقفل ملفات المستخدمين بحيث لا يمكن استعادتها. وقد عانى نحو 250 ألف فرد وشركة في أنحاء العالم بصمات كريبتولوكر، الذي عاد على مطوريه بما يقدر بـ 30 مليون دولار.

بل إنّ برمجيات الابتزاز المؤتمتة قد انتقلت إلى الهواتف النقالة مصيبةً مستخدمي أندرويد في بعض البلدان. ولم يكن الأفراد وحدهم من لسعهم سوط كريبتولوكر، بل ثمة أيضاً الكثير من الشركات والمنظمات غير الربحيّة بل وحتى الوكالات الحكوميّة، التي كان أشهرها قسم شرطة سوانسي في ماساتشوستس، الذي أصيب حين فتح أحد الموظفين ملفاً مرفقاً ببريد إلكتروني خبيث. وبدلاً من المجازفة بضياع ملفات قضايا الشرطة التي ليس لها بديل، أُجبرت الوكالة على فتح حساب بيتكوين لتسديد فديةٍ بلغت 75 دولار لاستعادة ملفاتها. وقد أخبر مساعد الشرطة غريغوري رايان بأنّه لم تكن لديه أية فكرة عن ماهية البيتكوين أو عن كيفية عمل البرمجيات الخبيثة إلى أن ضرب الهجوم القسم الذي كان يعمل به.

كما رأينا عبر هذا الفصل، فإنّ رحلةً إلى الهاوية قد تكون مظلمةً ومخيفة. لكن شركة الجريمة قد تمكنت ضمن هذا العالم من تطوير طرائق عملٍ في غاية التعقيد تساعدها على بيع كل شيء، من الميثاميتامين إلى البثّ الحي للاستغلال الجنسي للأطفال. وقد تبنت بسرعة أدوات إغفال الهوية، مثل تور، لتأسيس مراكز التسوق في الشبكة المظلمة. كما تتوفر خدمات استشارة إجرامية، كالاختراق واستئجار المرتزقة، يمكن الوصول إليها بنقرةٍ من الفأرة. وتشهدُ العملات الرقميّة مغفلة الهوية وغير القابلة للتتبع، مثل ليبرتي ريسيرف وبيتكوين، انطلاقةً جديدة ضمن اقتصاد العالم السري، وهي تسمح بالتبادل السريع للبضائع والخدمات. ومع توفر هذه العوائد الإضافيّة، تزداد شركة الجريمة انضباطاً وتنظيماً، مطورةً إلى حد كبير أساليب عملها. تتم أتمتة النماذج التجارية أينما أمكن ذلك بهدف أعظمة الأرباح، فالشبكات الروبوتية تستطيع تهديد التجارة العالمية الشرعيّة حيث يتم تدريبها بسهولة على أي هدفٍ تختاره شركة الجريمة. لقد تمّ الأمر في جوهره، وتمّ بناء آلة الجريمة. ومع وجود هذه الأنظمة قيد العمل، يُبين

عمق شركة الجريمة ومداها العالمي أنها تتمدد، بل وتتمدد أسّياً. بل إنّ هذا التهديد، وكأنه ليس سيئاً بما يكفي، سيصبح أسوأ بكثيرٍ بعد عندما نسلم شركة الجريمة المليارات من الأهداف الجديدة التي يمكنها مهاجمتها مع دخولنا عصر الحوسبة الكليّة المعروف باسم إنترنت الأشياء.

الفصل الثاني عشر
عندما تكون كل الأشياء قابلة للاختراق

ما زلنا في الدقائق الأولى من اليوم الأول لثورة الإنترنت.

سكوت كوك، شركة إنتيوت

حتى في عصر الإنترنت، قد يكون شراء سيارة عملاً مضنياً مقنطاً ومكلفاً في الوقت نفسه، بل إن المهمة ستصبح أصعب إذا كنت عاطلاً من العمل أو إذا كانت مواردك محدودة. لكن لحسن الحظ فإن مركز تكساس للسيارات في مدينة أوستن، يقدم خدماته لهذا النوع من الزبائن بالذات، واعداً الجميع بركوب سيارة، "لا يهم إن كان رصيدك الائتماني جيداً أو سيئاً، أو إن كنت مفلساً، أو كان البنك قد استحوذ على أملاكك، أو حتى إن لم يكن لديك أي رصيد ائتماني على الإطلاق." بالطبع عندما تكون الظروف قاسية، سيتأخر الناس عن تسديد دفعات قروضهم بالفعل، وسترتفع معدلات استعادة الملكية في بعض الوكالات إلى نسبة 45%. لم تكن استعادة ملكية السيارة يوماً بالأمر المسلي، سواء بالنسبة لأولئك الذين على وشك فقدان وسيلتهم الأساسية في التنقل، أو بالنسبة للتجار المضطرين لتوزيع أسطولٍ من مركبات القطر للبحث عن السيارة. فغالباً ما يتم إخفاء هذه السيارات عمداً من قبل أصحابها الذين يدركون أنهم على وشك إعادتها. وعندما يحضر المسترد مع قاطرته مطالباً بالسيارة يثور الغضب، فكثيراً ما ضُرب المستردون وطردوا، أو تم البصاق عليهم أو عضهم أو طعنهم بالسكاكين، أو حتى إطلاق النار عليهم حتى الموت، في سبيل استعادة ملكية التاجر. لا بد من وجود حل أفضل، ومركز تكساس للسيارات يعتقد أنه قد وجد مثل هذا الحل.

ابتاع المركز أداة تكنولوجية جديدة من شركة "باي تكنولوجيز" في كليفلاند، أملاً فيها أن تكون بديلاً أفضل بكثير من آلية المواجهة التي كانت

متبعة في الماضي عند استعادة الملكية. وكان منتج "باي تكنولوجيز" يعرف باسم "ويب تيك بلس"، وهو نظام يتيح لتجار السيارات تركيب "صندوق أسود صغير، بحجم رزمة من أوراق اللعب تقريباً، يخبّأ بذكاء تحت لوحة القيادة." يتم التحكم بهذه الأجهزة عن بعد، عبر موقع إلكتروني مركزي، ينقل الإشارات عبر شبكة لاسلكية إلى الصناديق السوداء الموجودة في السيارات. فعند تفعيلها، تسمح الإشارة للتاجر بأن "يُعطل نظام الاحتراق في السيارة، أو أن يشغل الزمور لتبدأ السيارة بالتزمير" إنها طريقة لطيفة وبالغة الدهاء لتذكير المالكين بأنهم تأخروا عن دفع مستحقاتهم. بدأ مركز تكساس للسيارات بتركيب هذه الأجهزة بالتدريج داخل كامل أسطول سياراته، وسرعان ما أصبح هناك نحو 1100 سيارة تملك هذا الجهاز داخلها. وكان عمر راموس - لوبيز هو المسؤول عن إدارة نظام الاسترداد الجديد عالي التقنية هذا، وهو جابي ائتمان شاب مولع بالتكنولوجيا يعمل في المركز.

بدا أن كل شيء يسير على ما يرام مع النظام الجديد حتى فبراير 2010، عندما توقفت عن العمل فجأة بضعة سيارات من مركز تكساس، ولم يكن من الممكن إعادة تشغيلها. لم يكن لدى أي شخص فكرة عن السبب، وقد بين تفقد سجلات الشركة أنّ جميع العملاء كانوا يدفعون المستحقات في موعدها. ومع مضي النهار، بدأ عدد الشكاوى بالارتفاع، وبحلول اليوم الخامس أغرق مئات العملاء الوكالة بالشكاوى الغاضبة. فما الذي كان يجري؟

لقد تعطلت سيارات العملاء في أنحاء مدينة تكساس فجأة، فبات من غير الممكن قيادتها أو إعادة تشغيلها. وفي منتصف الليل، بدأت مزامير السيارات بالتزمير عشوائياً في مدينة أوستن، وتم استدعاء الشرطة بسبب الكثير من شكاوى الإزعاج. وعندما وصلت الشرطة، اكتشفت أنه من غير

الممكن إيقاف المزامير من دون فصلها عن كابلاتها الموصولة ببطارية السيارة. وكان الأسوأ من ذلك أن مئات الزبائن وجدوا أنفسهم بلا وسيلة نقل مجبرين على عدم الذهاب إلى وظائفهم على الرغم من حاجتهم الماسّة لرواتبهم.

على الرغم من إهمال الحادثة في البداية على اعتبارها "عطلاً ميكانيكياً في النظام"، كان ثمة أمرٌ أفظع بكثير على وشك الوقوع. فقد دخل أحد المتطفلين خلسة إلى نظام تعطيل حركة السيارات عن بعد، الموجود على شبكة الإنترنت والتابع لمركز تكساس للسيارات، وبدأ بتعطيل السيارات الواحدة تلو الأخرى عبر المدينة مستهدفاً الزبائن. وباءت محاولات الوكالة لإعادة تشغيل السيارات بالفشل، وذلك لأن المخترق غيّر السجلات في قاعدة بيانات الشركة عبر تغيير أرقام تعريف السيارات وتبديل أسماء الزبائن الصحيحة بأسماء المشاهير، كمغني الراب الراحل توباك شاكور ونجمة البوب جينيفر لوبيز.

كان من الواضح أن شيئاً ما لم يكن في مكانه، وقد اتجهت الشبهات في النهاية نحو عمر راموس - لوبيز البالغ من العمر اثنين وعشرين عاماً، إذ كان قد تم فصله من الوكالة قبل أيام من حادثة شلل السيارات الواسعة الانتشار بسبب "عدم ملائمته لمعايير الشركة". وزعم مسؤولو السلطة التنفيذية أن راموس - لوبيز استغل معرفته بنظام مرؤوسيه السابقين واستخدم كلمة سر زميل سابق لينتقم لطرده، وذلك عبر تعطيل السيارات بشكل جماعي في مدينة أوستن. وأظهرت تحقيقات الشرطة أن جابي الائتمان السابق دخل إلى مخدمات "باي تيكنولوجيز" في أوهايو، عن طريق شبكة أيي.تي.أند.تي عريضة الحزمة التي تصل إلى بيته. وتم توقيف راموس - لوبيز واتهامه بارتكاب جناية خرق نظام حاسب.

أما بالنسبة لمركز تكساس للسيارات، فلم يكن قراره بتركيب تقنية

"المسترد عن بعد" في سياراته أمراً مميزاً، إذ توجد اليوم أكثر من مليوني سيارة تحمل هذه التقنية. لكن، كما سنرى لاحقاً في هذا الفصل، ثمة عشرات الملايين من السيارات حول العالم يمكن التحكم بها بطريقة أو بأخرى عن طريق الإنترنت، ناهيك بآلاف السيارات التي يتم ربطها يومياً بشبكة المعلومات العالمية. فبتركيب مثل هذه الصناديق السوداء داخل المزيد من السيارات، يتضح أكثر فأكثر أن قد يكون في سيارتك من الأبواب الخلفية أكثر مما كنت تتصور.

حيث توجد الأشياء اللاسلكية

عبر التاريخ القصير للحوسبة الحديثة، كنا نعتبر أن أجهزة الحاسب هي صناديق كبيرة من حجم ما. إذ كان جهاز الحاسب الواحد يحتل بناءً كاملاً في الخمسينيات. ومع قدوم السبعينيات، تم تقليص حجم جهاز الحاسب الكبير ليصبح بحجم البراد. وأتت الثمانينيات ومعها جهاز الحاسب المكتبي الشخصي، وقدّمت التسعينيات جهاز الحاسب المحمول. انتشر استخدام الهاتف المحمول في مطلع الألفية، وبحلول عام 2007 قدّم ستيف جوبز للعالم هاتف "آيفون"، وهو جهاز حاسب يحمل باليد، صغير لكن فعال. وتابع قانون "مور" مسيره كما دائماً. ولكن مفهومنا عما يمكن أن نسميه حاسباً سيتغير قريباً جداً، فالصناديق التي لطالما احتجزت المعالجات داخلها ستختفي لندخل عهد الحوسبة الكلية الوجود.

على عكس أجهزة حاسب الأمس المكتبية الثابتة، تَعد حقبة ما بعد جهاز الحاسب الشخصي بعالمٍ تتم فيه المعالجة الحاسوبية في أي مكان وفي كل الأشياء. فقد خلعت مبيعات الحاسب المحمول الحاسب الثابت عن عرشه منذ عام 2005. وبحلول عام 2015، سيتجاوز عدد الأجهزة اللوحية - كالـ "آيباد" - المباعة حول العالم، مبيعات الحاسبات الثابتة والمحمولة مجتمعة. ففي عام 2014، فاق عدد الهواتف المحمولة المستخدمة عدد

البشر على كوكب الأرض. ولدى الهواتف الذكية والأجهزة اللوحية في منازلنا شركاء بالطبع، فهي تترافق مع أنظمة ألعاب الفيديو ومسجلات الفيديو الرقمية وعلب الكابل والتلفزيونات الذكية، وجميعها متشابكة ومتصلة على الإنترنت. ولكن نزهة قصيرة في ممرات متجرٍ محلي للبيع بالتجزئة، مثل "بيست باي"، "لويز" أو "هوم ديبوت"، ستكشف أيضاً عن نزعة جديدة في طريقها للانتشار. حيث تتنافس مجموعة جديدة كاملة من الأجهزة الرقمية في هذه المتاجر، وفي كل مكان على الإنترنت، للحصول على حيزٍ لها في شبكات الإنترنت المنزلية. أشياء كموازين الحرارة والمصابيح الكهربائية ومكبرات الصوت وأجهزة مراقبة الطفل والأنظمة الأمنية المزودة بالإنترنت، تمثل جميعها الخطوات الأولى لنموذج جديد للحوسبة بدأ يظهر بسرعة ويعرف بإنترنت الأشياء، أو آي.أو.تي. عندما يسجل هذا النظام انطلاقته الحقيقية، فإنه قد يغير العالم الذي نعيش فيه تغييراً كبيراً مرةً وإلى للأبد.

يعرِّف مركز "يو" للأبحاث إنترنت الأشياء بأنه "بيئة محيطية متشابكة عالمية غامرة وغير مرئية للحوسبة، تشكلت عبر التكاثر المستمر لأجهزة الاستشعار والكاميرات والبرمجيات وقواعد البيانات الذكية ومراكز البيانات الضخمة، في نسيج من المعلومات يمتد على مستوى العالم".

كان أول من صاغ هذا المصطلح هو كيفين آشتون عام 1999، وهو باحث في معهد ماساتشوستس للتقانة، حيث لاحظ خلال عمله على مشروع لـ "بروكتر أند جامبل" أنه "إذا كانت كل أشياء الحياة اليومية مزودة بمعرّفات وبإمكانية الاتصال اللاسلكي، فسيمكن لهذه الأشياء أن تتواصل معاً وأن تتم إدارتها من قبل الحواسب... لو كان لدينا أجهزة حاسب تعلم كل ما يجب علمه عن الأشياء - باستخدام بيانات جمعتها هذه الأجهزة دون أية مساعدة منا - لكنّا سنتمكن من متابعة وحساب كل شيء، ومن

تقليل الهدر والخسارة والكلفة بشكلٍ كبير". لقد كان مفهوم "آشتون" بسيطاً وفعالاً، وكان له أثرٌ كبير على المصنعين وبائعي التجزئة، مثل "وولمارت"، في تحسين إدارة التوريد، وتخفيف التكاليف عن المستهلكين. إلا أن التكنولوجيا القادرة على جعل إنترنت الأشياء حقيقة، لم تكن موجودة عام 1999 خارج بيئات شديدة الإحكام، كالأنظمة الصناعية. لكن كل ذلك تغيّر اليوم، فقد اجتمعت مجموعة من التطورات معاً لتسمح بحصول قفزات كبيرة للأمام في عالم من الحوسبة الكلية الوجود، ولتسمح لأول مرة بانتشار واسع لـ "أجهزة الحاسب المصغرة المدمجة في الأشياء والمرتبطة بالإنترنت بواسطة تقانة لاسلكية." وبالفعل، فإنه وفقاً لجمعية صناعة أشباه النواقل، أصبح الناس في عام 2004 يصنعون الترانزستورات بكمية أكبر من حبات الأرز وبكلفة أدنى.

لقد أصبح من الممكن بفضل التطورات التي شهدتها الدارات الكهربائية والبرمجيات وإمكانيات التصغير، بناء إنترنت الأشياء والذي يمكن تصنيف أجهزته وفق مجموعتين: أجهزة الاستشعار وأجهزة التحكم الدقيقة. فأجهزة التحكم الدقيقة هي عبارة عن معالجات حواسيب قابلة للبرمجة يبلغ قطرها بضعة ميلمترات فقط. إنها رقاقات حاسب رخيصة جداً ومنخفضة الطاقة، بعضها لا يزيد حجمه عن حجم رأس الدبوس، ويمكن بناؤها ودمجها بعدد لا نهائي من الأجهزة، وبعضها لا يكلف سوى بضعة بنسات. لا تحتاج أجهزة الحوسبة الصغيرة هذه إلا لبضعة ميليواطات من الكهرباء، ويمكنها وبالتالي العمل لسنوات معتمدة على بطارية ضئيلة أو على خلية شمسية صغيرة. نتيجة لذلك، أصبح من الممكن صنع "مزود شبكة، يمكن حمله على (أو داخل) طرف الإصبع مقابل دولار واحد".

ستستقبل هذه الرقاقات الدقيقة البيانات من مجال شبه لا نهائي من أجهزة الاستشعار، وهي أجهزة دقيقة قادرة على مراقبة أي شيء يمكن

قياسه وتسجيله، مثل الحرارة، الطاقة والموقع وتدفق المياه والإشعاع والضغط الجوي والتسارع والدوران والقوة المغناطيسية والارتفاع والصوت والفيديو. وستسمح لنا هذه المجموعة الشاملة من أجهزة الاستشعار بفهم وتحليل العالم المحيط بنا والتفاعل معه كما لم تستطع قدراتنا البشرية من قبل. ولن تبقى هذه البيانات بلا استخدام، فبعد جمعها ستتم معالجتها من قبل مجموعة جديدة من أجهزة التحكم الدقيقة في إنترنت الأشياء كالمذكورة أعلاه، كالفاصلات المصغرة والمحركات والصمامات والماكينات والتوربينات والمولدات، وكلها قادرة على التفاعل بشكلٍ مستقل مع العالم المادّي المحيط بنا. بالتالي، عندما يميز جهاز الاستشعار حرارةً أو ضغطاً زائداً في أنبوب الغاز على سبيل المثال، سيكون المتحكم الدقيق الخاص به والمستقبل للمعلومات مبرمجاً للاستجابة بالإغلاق أو تحويل مسار تدفق الغاز الطبيعي، وبالتالي الحيلولة دون وقوع انفجار كارثي.

سيسمح النمو الأفقي في شبكات البيانات اللاسلكية العالية السرعة لأجهزة الاستشعار هذه بأن تتحدث إلى العالم باستخدام مجموعة متنوعة من تقنيات وبروتوكولات الاتصال كالوايفاي والحزمة العريضة وجي.إس.إم (النظام العالمي للمواصلات الجوالة)، وسي.دي.إم.إي (الوصول المتعدد عبر تقسيم الشيفرة)، والبلوتوث ومعرفات الهوية الراديوية وإن.إف.سي (التواصل القريب المدى)، وزيج.بي وموجات زد وخطوط القدرة الكهربائية. ولن تتواصل هذه الأجهزة مع شبكة الإنترنت الأوسع وحسب، بل مع بعضها البعض أيضاً، لتولد كمية عصية على الفهم من بيانات آلة - لآلة، والتي سيتم تخزينها ومعالجتها بسرعة أكبر وبكلفة أقل بفضل الحوسبة السحابية وقدرتها شبه اللامحدودة على تخزين البيانات. وستكون النتيجة "بيئة محيطية متشابكة، عالمية، غامرة وغير مرئية للحوسبة"، وما هذا كله سوى مقدمة لموجة عارمة من التغيير الذي سيأتي لاحقاً.

على أي حال، ثمة شيء واحد لا بد من إصلاحه أولاً، وهو بروتوكول الاتصالات الأساسي، الذي يوجه أغلب عمليات النقل على الإنترنت. فالعمود الفقري للإنترنت اليوم يعمل بالاعتماد على ما يسمى النسخة الرابعة من بروتوكول الإنترنت آي.بي4. فالهندسة المعمارية الحالية للاتصالات موجودة منذ عام 1981، وهي تؤمن نحو 4.3 بليون عنوان شبكة منفصل يمثل كل منها جهازاً متصلاً. عندما تم تقديم الإصدار الرابع من بروتوكول الإنترنت في نهاية السبعينيات لم يكن أحد يتصور أن 4.3 بليون عنوان لن تكون كافية لتلبية متطلبات العدد المحدود جداً من الجامعات والشركات التي كانت متصلة بالشبكة آنذاك. أما اليوم، فقد وقع ما لم يكن متوقعاً بالأمس، إذ نفدت عناوين الإنترنت. وكما حدث عندما احتاجت مدينة نيويورك لإنشاء رموز جديدة للمناطق بعد أن نفدت أرقام الهواتف البالغ عددها 212 التي كانت تخدم سكانها، كذلك كان الأمر مع الإنترنت.

جاء رد الإنترنت على هذه المشكلة عبر الإصدار السادس لبروتوكول الإنترنت، الذي سيحل محل إصداره الرابع ليزيد فضاء العناوين المتاح على الشبكة زيادة كبيرة. ويحل البروتوكول الجديد المشكلة بزيادة طول "رقم الهاتف" من 32 بايت إلى 128 بايت. رياضياً، لا يمكن للإصدار الرابع دعم أكثر من 232 أو 4.3 بليون اتصال. أما الإصدار الرابع فيوفر 2128 أو 34 اتصالاً. مضاعفات هذا الرقم مربكة للذهن. فهناك 1019 حبة من الرمل في كل شواطئ العالم. وهذا يعني أن الإصدار السادس سيسمح لكل حبة رمل أن يكون لها ترليون عنوان إنترنت. وبالفعل، يوجد من العناوين الممكنة مع لإصدار السادس لبروتوكول الإنترنت ما "يمكننا من إنشاء عناوين إنترنت لكل ذرة على سطح الأرض، وسيبقى لدينا عناوين تكفي لـ 100 كرة أرضية أخرى وأكثر". ستكون هذه التغييرات كلها هي المقدمة لولادة إنترنت الأشياء.

للمساعدة على فهم هذه الأرقام الضخمة، يمكننا أن نعتبر مجازاً أن حجم الإنترنت اليوم يعادل حجم كرة غولف، عندها سيكون إنترنت الغد بحجم الشمس. وهذا يعني أنه لن يكون خلال السنوات القادمة كل حاسوب وهاتف وجهاز لوحي موصولاً بالإنترنت فقط، بل أيضاً كل سيارة، ومنزل وكلب وجسر ونفق وخط أنابيب ودمية وعلبة صودا. وإذا كان هناك ثلاثة عشر بليون جهازٍ متصلٍ بالإنترنت عام 2013،، فإن شركة سيسكو للأنظمة تقدر أنه بحلول عام 2020 سيصبح هناك خمسون بليون شيء متصل بالإنترنت، مع مساحة كافية للنمو التوسعي بعد ذلك. وعندما تصبح كل هذه الأجهزة متصلة بالإنترنت، وتبدأ بمشاركة البيانات مع بعضها البعض، سيؤدي ذلك لتحسن كبير في الخدمات اللوجستية وكفاءة الموظفين وعمليات سلسلة التوريد واستهلاك الطاقة، وخدمة الزبائن، والإنتاجية الشخصية.

كما سبق أن نوهنا، ينص قانون ميتكالف على أن قيمة شبكة ما تزداد أسياً مع ازدياد عدد العقد أو الحاسبات المتصلة بها. وعندما سيضيف الإصدار السادس من بروتوكول الإنترنت 340 أوندسيليون (340 ترليون ترليون ترليون) عقدة محتملة جديدة لشبكة المعلومات العالمية، سيكون انفجار القيمة الاقتصادية المرافق لذلك عصياً على الحصر. وتتنبأ مؤسسة ماكنزي العالمية بأن تضخ الابتكارات التي ستصبح ممكنة عبر قطاعات متعددة بفضل إنترنت الأشياء بنحو 6.2 ترليون إضافية لقيمة الاقتصاد العالمي بحلول عام 2025. ومن الوارد جداً أن تصبح إنترنت الأشياء موجودة حيث يوجد أقرب فايسبوك أو غوغل أو آبل، كما أن عدد أجهزة الاستشعار وأجهزة المستهلك وأجهزة التحكم الصناعية المتصلة بالإنترنت قد تجاوز بالفعل عدد الهواتف المحمولة. ولقد كان للابتكارات السابقة لإنترنت الأشياء مثل الأجهزة الرياضية المحمولة من فيتبيت وجوبون

ومعدات الحقيقة الافتراضية من أوكولوس ريفت وساعات ويثينغز وشرائح التقفي من إيستيموت، وأجهزة صوت سونوز صدىً واسع وقيمة سوقية كبيرة. بل إن إحدى هذه الشركات، وهي شركة نيست لابس لموازين الحرارة الذكية، تم استحواذها فجأة عام 2014 مقابل 3.2 بليون دولار بعد 854 يوماً فقد على إطلاق منتجها الأول. وإذا كان ما من شك في إمكانية ربح الكثير من المال عير إنترنت الأشياء، فإن آثارها الاجتماعية قد تتجاوز أثرها الاقتصادي.

تخيُّل إنترنت الأشياء

> إنترنت الأشياء هي طريقة للقول إن أشياء أكثر في العالم ستصبح جزءاً من الشبكة... إننا ندمج العالم أكثر فأكثر ضمن جهاز الحاسب
>
> جوردون بل، باحث في مايكروسوفت

تبدو وعود إنترنت الأشياء وعوداً وردية. فبما أن الرقاقات وأجهزة الاستشعار سيتم دمجها بأغراض الحياة اليومية، ستصبح لدينا معلومات ووسائل راحة أفضل في حياتنا. فحين يكون منبّهك متصلاً بالإنترنت على سبيل المثال سيتمكن من الدخول إلى مفكرتك الرقمية وقراءتها، وسيعرف متى وأين سيكون موعدك الأول خلال اليوم، وسيكون قادراً على مطابقة مصادر المعلومات مع آخر أحوال حركة السير. فإذا كان الازدحام خفيفاً، ستتمكن من النوم لعشر دقائق إضافية، وعند الازدحام الشديد قد تجد نفسك تستيقظ أبكر مما كنت تأمل. وعندما ينطفئ المنبه بالفعل، سيقوم بتشغيل الأضواء في المنزل برفق، وربما سيشغل التدفئة ويعدّ لك حمامك. ستنفتح فتحة الحيوانات المنزلية تلقائياً، لتدع "فيدو" يخرج إلى الفناء الخلفي ليقوم بجولته الصباحية، والأهم من ذلك هو أن آلة صنع القهوة ستبدأ بتحضير أول فنجان قهوة لك بالوقت المناسب. ولن تضطر لأن تسأل أطفالك إن كانوا قد نظفوا أسنانهم، فالرقاقة داخل فرشاة أسنانهم سترسل

رسالة لهاتفك الذكي لتُعلمك بأن المهمة قد تمت. ولن تقلق بشأن العثور على مفاتيحك أثناء خروجك من الباب، فجهاز الاستشعار المزود بمرشد لاسلكي في سلسلة المفاتيح سيجعل تحديد موقعها في منزلك ممكناً بالإشارة إلى دائرة نصف قطرها 2 بوصة. لقد بدأت أخيراً حقبة "آل جيتسون".

بينما كان مقياس الحماسة الخاص بإنترنت الأشياء يومض بالأحمر لبعض الوقت، بات كل ما تم وصفه أعلاه ممكناً تقنياً اليوم. ولا شك في أنه ستكون ثمة عقبات، وبالأخص تلك المتعلقة بغياب المعايير التقنية المشتركة، لكن مجموعة كبيرة متنوعة من الشركات والجمعيات ووكالات الحكومات تعمل بجد لجعل إنترنت الأشياء حقيقة واقعة. وستكون النتيجة هي انتقالنا من مرحلة الاتصال لمرحلة فرط الاتصال، وككل الأمور التي يذكرها قانون ميتكالف، ستصبح هذه النتيجة واقعاً قبل حتى أن نلاحظ ذلك. وستؤثر الحوسبة الكلية الوجود على كل مجال من مجالات التطور البشري، بما فيها النقل والطاقة والتمويل والحكم والزراعة والتعليم والسلامة العامة والسفر والتجارة.

إن إنترنت الأشياء تعني أن كل الأشياء المادية في المستقبل ستكون مزودة بعنوان إنترنت، وسيتم تحويلها إلى تكنولوجيا معلوماتية. نتيجة لذلك، سيصبح مصباحك وقطتك وشجيرة اللبخ الخاصة بك جزءاً من شبكة تكنولوجيا المعلومات. والأشياء التي كانت صامتة في ما مضى سيصبح لها صوت، وسيصبح كل غرضٍ قادراً على الإفصاح عن قصته وتاريخه الخاص. وسيعلم البرّاد بالضبط تاريخ صنعه، وأسماء الأشخاص الذين قاموا بصنعه، والمصنع الذي أتى منه، واليوم الذي غادر فيه خط التجميع ووصل فيه إلى بائع التجزئة، ثم انضم إلى شبكة منزلك. سيقوم البراد بتسجيل كل مرة تم فيها فتح بابه أو نسي فيها طفل من أطفالك أن يغلقه. وعندما يبدأ أي عطل في محرك البرّاد، سيعطي إشارة طلباً للمساعدة. وعندما يتعطل

المحرّك كلياً، سيخبرنا البرّاد كيف يمكن تفكيك قطعه وتدويرها بأفضل طريقة. وستعرف الأبنية كل شخص عمل فيها، وستعرف المنازل كل شخص عاش فيها، وستعرف مصابيح الشوارع كل سيارة مرت بها.

ستتواصل كل هذه الأشياء مع بعضها، وستكون قادرة على تسخير القوة الضخمة للمعالجة والتخزين التي تملكها السحابة، والتي تم تحسينها عبر شبكات اجتماعية ونقالة إضافية. سنعيش في عالم يكون كل شيء فيه قابلاً للبرمجة وقادراً على التفاعل. ستصبح الأشياء "ذكية"، وستكون قادرة على وصف موقعها وقربها وسرعتها وحرارتها وتدفقها وتسارعها والأصوات المحيطة بها، وما تراه والقوى الفاعلة في وسطها والحمل الواقع عليها وعزم الدوران والضغط والتفاعلات التي تشهدها. وإذا كان الجيل الأول من الهواتف الذكية، والموازين الذكية، والساعات الذكية، والبطاقات الذكية موجوداً اليوم، فإن الأشياء في المستقبل ستصبح كلها ذكية، بل إنها ستصبح أكثر ذكاء بكثير مما هي عليه اليوم. وستطور هذه الأجهزة نوعاً خاصاً من الحساسية عندما تتصل معاً، وسينتج عن ذلك عالم تلتقي فيه الأشياء والبيانات والناس معاً. وسنرى نتيجة لقوة الحوسبة المدمجة "مليارات الأشياء الذكية المتصلة مع بعضها"، تنضم لشبكة عالمية عصبونية في السحابة التي "ستؤثر على كل جانب من جوانب حياتنا".

في الوقت الذي كانت فيه الإنترنت "القديمة" تسمح للحاسبات المحمولة والثابتة والمخدمات بمشاركة المعلومات، ستتيح الإنترنت "الجديدة" إمكانية التحكم عن بعد بأي شيء على سطح الأرض. فكما يوضح لنا جوي آيتو، مدير مختبر الإعلام في معهد ماساتشوستس للتقانة، هناك "ظاهرة من التقارب حيث تندمج البتات الآتية من المملكة الرقمية مع الذرات الموجودة في عالمنا المادي." سيكون لكل شيء هوية وحياة في كلا العالمين الافتراضي والمادي، وعندما يحدث ذلك، سيزول الفرق بين الاتصال بالشبكة

وعدم الاتصال بها، هذا الفارق الذي كان مهماً حتى وقت قصير. بل إن المدير التنفيذي لشركة سيسكو جون شامبرز، تنبأ مؤخراً بأن يكون لإنترنت الأشياء أثر يبلغ خمسة إلى عشرة أضعاف أثر الإنترنت نفسها.

سيصبح من الممكن فجأة في هذا العالم معرفة ما كانت تستحيل معرفته في السابق. إذ سيتم تعقب السلع بدءاً من الحقل وحتى طاولة الطعام، وستحتفظ المطاعم بمدخلات عن كل صحن تتضمن محتواه، من أكل منه، وكم هي سرعة النوادل في نقله من المطبخ إلى الزبون. وهكذا، إذا ما تفشى وباء الإشريكية القولونية مرة أخرى، لن نضطر لإغلاق خمسمئة مطعم ولن نتساءل ما إذا كان سبب المشكلة هو لحم الدجاج أم البقر. فسوف نعلم بالضبط مع أي مطعم، ومزود، وحافلة طعام علينا أن نتواصل لحل المشكلة بسرعة. ستخلق إنترنت الأشياء والبلايين من أجهزة الاستشعار التابعة لها، شبكة ذكية محيطة تربط وتحسّ وتشعر وتساهم بشكل كبير في خلق كون قابل للفهم.

لن يصبح من الممكن معرفة ما كانت تستحيل معرفته في السابق وحسب، بل سيصبح المستحيل فجأة ممكناً. والأشياء التي كانت تعتبر منطقية لن تعود كذلك، كأجهزة الكشف عن الحرائق على سبيل المثال. إذ لماذا لا تقوم معظم أجهزة الكشف عن الحرائق سوى بالصفير بقوة عندما تكون حياتك معرضة لخطر الموت بسبب النيران؟ في المستقبل، ستشغّل هذه الأجهزة أنوار غرفة نومك لتوقظك، وستشغل نظام الصوت في منزلك ليشغل ملفاً صوتياً يحذر بصوت عالٍ، "حريق، حريق، حريق"، بل إنها ستتصل أيضاً بقسم المطافئ وبجيرانك (في حال كنت فاقداً للوعي أو بحاجة للمساعدة)، وستقطع تلقائياً التدفق عن أجهزة الغاز في المنزل. لن تكون الوحيد الذي قد تنقذ إنترنت الأشياء حياته، فهي ستنقذ حياة لنباتاتك أيضاً. فأجهزة استشعار الرطوبة الرخيصة الموضوعة في تربة

النباتات تستطيع منذ عام 2009 استخدام شبكة الوايفاي المنزلية لترسل تغريدات تصرخ فيها: "عاجل! اسقني!".

لم يكن ذلك مستقبلياً بما يكفي؟ ماذا عن إنترنت بين - نوعية تصل الأفيال والدلافين والقردة الكبيرة "بهدف التقوية، والبحث، والحماية"؟ قد يبدو ذلك مجنوناً، لكنه موجود بالفعل. ففي أستراليا على سبيل المثال، هناك نحو 300 سمكة قرش على تويتر. لا، لم تقم بإنشاء حساباتها بنفسها، بل قام باحثون بوسم 338 سمكة قرش، بما فيها العديد من أسماك القرش الكبيرة البيضاء، بشرائح صوتية ترسل إشارات إلكترونية إلى مستقبلات متمركزة على الشاطئ عندما تقترب هذه الأسماك لمسافة نصف ميل من السواحل. فبالنسبة لبلدٍ عانى هجمات القرش القاتلة أكثر من أي بلدٍ آخر، من شأن هذا التطور نحو إنترنت الأشياء أن ينقذ حياة البشر، بينما جذبت أسماك القرش نحو أربعين ألف متابع على التويتر من مرتادي الشواطئ.

سيكون المنتج الجانبي لإنترنت الأشياء عبارة عن شبكة معلومات عالمية حية تتنفس، وستصبح التكنولوجيا حيةً بطرق لم نشهدها من قبل، كما في أفلام الخيال العلمي. وبينما قد يبدو هذا المستقبل بعيد المنال، فإن الاتصالات في ما بين الآلات قد تجاوزت بالفعل في حجمها جميع النشاطات البشرية الأصل على الإنترنت، ففي نهاية عام 2013 أصبح أكثر من 61.5% من حركة الإنترنت عبر العالم تنتج عن الأشياء. وبينما نشق طريقنا باتجاه الحوسبة الكلية الوجود، ستفوق نتائج هذه الظاهرة ومضاعفاتها على الأرجح جميع تصوراتنا. مثلما كان دخول الكهرباء مدهشاً في حينه، لكنها توارت في نهاية المطاف لتصبح في الخلفية وسيطاً غير محسوس ومنتشراً في كل مكان يضمن تواصلنا المستمر مع العالم المادي. لكن قبل أن ندع هذا يحدث، ونظراً لكل هذه الوعود التي أتت بها إنترنت الأشياء، علينا أن نطرح أسئلة ذات أهمية حاسمة حول هذا العالم الجديد الجريء. فبينما

تبدو فوائد إنترنت الأشياء متعددة الوجوه وواضحة، يضعنا إنترنت كل الأشياء أمام مخاطر جمة. وكما يمكن للكهرباء أن تصعق وتقتل، كذلك الأمر بالنسبة لبلايين الأشياء المتشابكة والمتصلة مع بعضها وبالإنترنت.

ربط كل شيء - بطريقة غير آمنة

وصل الأشياء بالإنترنت سيكون بمثابة كهربة القرن الحادي والعشرين.

مات ويب، المدير التنفيذي لشركة بيرغ كلاود

لكي تتصل الأشياء بالإنترنت وتتواصل في ما بينها، يجب أولاً تمكينها من التكلم عبر معادل تكنولوجي مناسب. فكما رأينا في مركز تكساس للسيارات وفي تقنيات كالصندوق الأسود من ويب.تيك.بلس، يمكن للسيارات أن "تتكلم" بالفعل، لتصرخ مصرحة عن بيانات موقعها وحالتها وظروفها. فمنح أشياء الحياة اليومية القدرة على التحدث معنا ومع بعضها، يقع في جوهر تحقيق الرؤية التي يصبو إليها أنصار إنترنت الأشياء.

ولكي يتم تحقيق ذلك، تعتمد إنترنت الأشياء على سلسلة من تقانات وبروتوكولات الاتصال المتنافسة. ستوصل معايير بث البيانات النقالة والخلوية، مثل إل.تي.إي وفور.جي وسي.دي.إم.إي الأجهزة بشبكة الهاتف المحمول. وستتمكن العديد من الأشياء الكبيرة من التواصل عبر خطوط ثابتة سلكية كما في شبكات الإيثرنت والألياف البصرية. ولكن أسباب السعر وسهولة التعامل قد تدفع أكبر عدد من الاتصالات إلى الشبكات اللاسلكية. وستكون النتيجة بلايين الرقاقات المدمجة في أغراض تستخدم معايير مثل الوايفاي والبلوتوث وزيجبي وموجات زيد والتواصل القريب المدى ومعرفات الهوية الراديوية بغرض التواصل. وبالتزامن مع انخفاض سعر هذه الأدوات، قد تصبح منتجات استهلاكية جديدة مثل آي.بيكون من آبل وواسمات الموقع من تايل ميزة منتشرة في حياتنا اليومية، متيحةً لنا تعقب الأشياء بدقة تصل لمستوى السنتمتر.

لقد حازت أولى التقانات التي تدعم إنترنت الأشياء، وهي نظام آر.إف.آي.دي أو معرفات الهوية الراديوية، براءة اختراع عام 1983، وهي عبارة عن جهاز لاسلكي منخفض الطاقة يمكن دمجه بأي شيء لجعله "ذكياً"، أو يمكنه التفاعل مع قارئات آر.إف.آي.دي. وواسمات آر.إف.آي.دي هي عبارة عن دارات إلكترونية مطبوعة تعادل سماكتها سماكة ورقة. وهي غالباً ما توجد على شكل ملصق بحجم عملة العشرة سنتات، ويمكن إنتاجها بكلفة لا تتجاوز السنت الواحد. إنها قادرة على تبادل البيانات الثابتة فوراً، ويمكن قراءتها بوساطة الماسحات الضوئية من مسافة تصل في بعض الأحيان إلى المئة متر. وحتى إذا لم تكن تقانة معرفات الهوية الراديوية مألوفة لك من قبل، فهناك احتمال كبير بأنك قد تعاملت معها في حياتك، سواء كانت بطاقة التعريف الأمنية التي تستخدمها لتصل إلى مكتبك، أم بطاقة ائتمان "لوّح وادفع"، أو مفتاح غرفتك في الفندق، أو بطاقة المرور لمترو الأنفاق، أو الصندوق الصغير الذي تستخدمه لدفع رسوم الطرق السريعة، مثل إي.زيد.باس. وبالرغم من الراحة العظيمة التي يؤمنها نظام معرفات الهوية الراديوية، والذي يعتبره كثيرون بوابة إنترنت الأشياء، إلا أن هناك مشكلة واحدة: إنه قابل للاختراق بشكل كبير.

هنالك الكثير من الهجومات التي استهدفت تقنية معرفات الهوية الراديوية، والتي يمكن اختراق إلكترونياتها بسهولة أو تشويشها أو محاكاتها، كما أنه يوجد "وسط سري" فاعل متخصص بمعرفات الهوية الراديوية يعمل باستمرار على تحسين تقنيات الهجوم هذه. إن الأغلبية الساحقة من هذه الواسمات لا تتمتع بأي أمن أو تشفير أو بروتوكولات خصوصية فعالة. وقد أتاحت هذه العيوب للهاكر فرانسيز براون أن يصنع قارئات آر.إف.آي.دي خاصة به بأقل من 400 دولار، يمكنها أن تمسح ضوئياً وتنسخ وتستنسخ وتسرق البيانات من بطاقاتك الذكية. فبينما تقف أنت في

الطابور في محل البقالة، أو تجلس في مقطورة مزدحمة في مترو الأنفاق، أو تركب المصعد لتصل لمكتبك، أو تنتظر قهوتك الصباحية في مقهى ستاربكس، يمكن لبراون أن ينفذ هجوم "تمرير الفرشاة". وبينما يقف هناك مبتسماً وربما مدردشاً معك، ستستعلم قارئة آر.إف.آي.دي المحمولة المخبأة في حقيبة ظهره عن بطاقة مفتاح المكتب التي تضعها في محفظتك أو جيبك أو حقيبتك وسيفرّ بكل التفاصيل المرمزة عليها. فما المشكلة في ذلك؟

إليكم المشكلة: يمكن لبراون بعد ذلك أن يوصل قارئة آر.إف.آي.دي الخاصة به بحاسبه في المنزل، وأن يستخدمها ليستنسخ معرفات هوية راديوية مناسبة طوال اليوم، وهذا يعني أنه يمكنه الدخول لمكتبك، أو غرفتك في الفندق، أو منزلك في أي وقت يحب. تستخدم كل شركات "فورتشن 500" في أميركا نظام آر.إف.آي.دي في شارات موظفيها لتتحكم بالدخول إلى مباني مكاتبها، ولدى براون نسبة نجاح تبلغ 100% في استنساخ هذه البطاقات. إن عواقب هذا الأمر هائلة، فهي تنسحب على كل شيء بدءاً من التجسس الصناعي وصولاً إلى عمليات السطو الشائعة وسلامة الموظفين. إن الاعتماد على معرفات الهوية الراديوية غير الآمنة باعتبارها النظام الأساسي الذي نستخدمه في إجراءات الأمن والتعريف بالهوية في مكان العمل، يعني أن النظام الحالي منهار تماماً. والأسوأ من ذلك بعد هو أن هذه البطاقات لا يمكن تحديثها بسهولة بتحميل برنامج جديد كما تفعل مع حاسبك المنزلي، بل لا بد من استبدال كل واحدة منها، وهو اقتراح مكلف بالنسبة لشركة تملك 100000 موظف.

حتى لو كنت لا تستخدم بطاقة آر.إف.آي.دي في عملك، هناك احتمال كبير بأنها لديك أو أنها ستصبح لديك قريباً بدمجها ببطاقتك الائتمانية القابعة في محفظتك. والتي تمكن المخترقون من الولوج إليها أيضاً باستخدام

قارئات آر.إف.آي.دي رخيصة موجودة على موقع إي.باي مقابل 50 دولاراً فقط، وهي أدوات تسمح للمعتدي بالتقاط رقم بطاقة ائتمان الهدف وتاريخ انتهاء صلاحيتها ورمز الأمان الخاص بها. وبعد ذلك بلحظات، وباستخدام أداة لمغنطة البطاقات تكلف 300 دولار، يمكن إعادة كتابة تلك البيانات على بطاقة جديدة، وبهذا يمكن للمحتال أن يبدأ بعمليات الشراء التي يمكن إنجازها خلال عدة دقائق فقط. أهلاً بكم في عالم النشب في إصداره الثاني، حيث لن يضطر اللصوص لأن يحشروا أيديهم في جيبك بعد الآن.

من السهل محاكاة تقنيات اختراق معرفات الهوية الراديوية، فمئات المواقع التعليمية والفيديوهات على الإنترنت تعلّم المخترقين بالضبط كيف يقومون بذلك. وهذا أمر مثير للقلق، فبلايين الأشياء التي ستتصل بالإنترنت ستستخدم معرفات الهوية الراديوية كلغتها الأساسية للكلام والتفاعل مع العالم. ويمكن لهذه الرقاقات أن تصاب بالفيروسات، كما أنه يمكن تشويش إشاراتها مثلما يمكن ذلك مع إشارات جي.بي.إس، لمنعك من الوصول إلى مكتبك وللسماح للصوص بسرقة البضائع الثمينة الموسومة إلكترونياً لدى بائعي التجزئة. توجد تقنية اتصال أخرى مشهورة من إنترنت الأشياء، وتعتبر الأخ الأصغر لمعرفات الهوية الراديوية، تعرف باسم اتصال الحقل القريب، وقد تم تضمينها داخل 20% من الهواتف المحمولة، وبخاصة نماذج أندرويد. هناك العديد من الاستخدامات لاتصال الحقل القريب، ولكن أكثرها شيوعاً هو خدمات الدفع على الهاتف المحمول مثل "محفظة غوغل".

ليس عليك سوى أن تمرر هاتفك أمام قارئ اتصال حقل قريب لكي تدفع ثمن منتج ما، وسيتم حسم الأموال من محفظة هاتفك الافتراضية، أو سيتم إرسالها إلى بطاقة ائتمانك. ولكن على غرار معرفات الهوية الراديوية، تم

اختراق اتصالات الحقل القريب في عدة حالات بوساطة تطبيقات اختراق مثل إن.إف.سي.بروكسي القادر على نسخ بيانات بطاقة الائتمان عبر اتصال الحقل القريب بشكل فوري لإعادة إرسالها لاحقاً بحيث يستخدمها الرجل الشرير لشراء البضائع والخدمات التي يختارها بنفسه. لقد تم اختراق محفظة غوغل مراراً عبر قراءة رقم التعريف الشخصي بدون إذن أو الوصول إلى الرصيد المخزّن في هاتفك. والآن، بما أن آي.فون ستتيح إمكانية الدفع بالهاتف المحمول مع تطبيق آبل.باي، من المرجح أن يتحول انتباه المجرمين إلى الالتفاف على أنظمة أمان آبل أيضاً.

وفي حادثة أخرى، استطاع أحد المخترقين استهداف رقاقة اتصال حقل قريب في هاتف محمول قريب ليسيطر على الجهاز ويجري اتصالات هاتفية ويرسل رسائل نصية ويدخل إلى الملفات، كل هذا دون معرفة المالك الحقيقي للجهاز. وتستخدم تطبيقات اتصال الحقل القريب على الهواتف المحمولة منذ اليوم للتسديد في أنظمة النقل الداخلية، وقد اخترق المحتالون في سان فرنسيسكو ونيوجيرسي بوابات اتصال الحقل القريب باستخدام تطبيق يسمى ألترا.ريسيت، يقوم تلقائياً بتسديد أية أجور تطلبها مشغلات القطارات، ما يعني ركوب مترو الأنفاق مجاناً مدى الحياة.

ثمة تقنية اتصال لاسلكية أخرى من إنترنت الأشياء كانت قد ارتفعت معدلات استخدامها وشهرتها وهي البلوتوث، ولكن تم تخريبها بسهولة مثل ما حدث مع تقنيتي معرفات الهوية الراديوية واتصال الحقل القريب. فهناك العديد من التطبيقات والبرامج المجانية سهلة الاستخدام مثل بلو.سكانر، وبلو.باغر، وبي.تي.بروسر، وبلو.سنيف تسمح لأي شخص خبيث أن يتصل بسهولة بجهاز مزوَّد بتقنية البلوتوث ليتحكم به. تمكن هذه الأدوات من الدخول دخولاً غير شرعي إلى الأجهزة بطريقة تسمى "بلو سنارفينغ" للوصول عبر منفذ البلوتوث لأي بيانات مخزنة على الهواتف

الذكية أو الحاسبات المحمولة أو الثابتة. بل إن بإمكان المهاجمين أيضاً اعتراض البيانات التي تكتبها على لوحة مفاتيحك اللاسلكية أو قراءة رسائلك النصية والتقاط صور بدون علمك، وحتى التجسس على سماعات البلوتوث الخاصة بك بينما تجلس في المطار منتظراً.

"حمّى إنترنت الأشياء" قادمة إلينا لا محالة، وما من طريق عودة. وإذا كان لربط كل شيء بإنترنت الأشياء العالمي قيمة عظيمة، فإن ربط الأشياء بشكل غير آمن ليس كذلك. وقبل أن نضيف بلايين الأشياء القابلة للاختراق، وقبل أن نتصل بوساطة بروتوكولات نقل بيانات قابلة للاختراق، هناك أسئلة مهمة يجب طرحها حول المخاطر المرافقة، مع أخذ الآثار المتزايدة لمستقبل الأمن والجريمة والإرهاب والحرب والخصوصية في الاعتبار.

طمس الخصوصية

> سيتم تحديد موقع المواد الهامة والتعرف عليها ومراقبتها والتحكم بها عن بعد عبر تقنيات مثل معرفات الهوية الراديوية وشبكات المستشعرات والمخدمات المدمجة الصغيرة وحاصدات الطاقة - وكلها متصلة مع الجيل الثاني من الإنترنت باستخدام الحوسبة الغزيرة العالية الطاقة المنخفضة الكلفة.
>
> ديفيد بيتريوس، مدير متقاعد لوكالة الاستخبارات المركزية

الطريقة نفسها التي يتم بها اليوم تعقب وتسجيل وبيع كل خطوة نقوم بها على الإنترنت وتحويلها إلى نقود، سيصبح ذلك ممكناً في المستقبل القريب في العالم المادي أيضاً. سيصبح الفضاء المادي مماثلاً تماماً للفضاء الافتراضي، وعندما تنضم كافة الأشياء المحيطة بنا لإنترنت الأشياء، سيزول أي فرق مهم بين العالم الشبكي والعالم غير الشبكي.

ومع الانتشار الواسع للأجهزة المتصلة بشبكة الإنترنت، سيتعرّض كل ما يفعله الناس في منازلهم وسياراتهم وأماكن عملهم ومدارسهم ومجتمعاتهم

لمزيد من المراقبة والتحليل من قبل الشركات التي تقوم بتصنيع هذه الأجهزة. وستتم بالطبع إعادة بيع هذه البيانات للمعلنين وسماسرة البيانات والحكومات على حد سواء، ليتم لهم بذلك اطلاع غير مسبوق على حياتنا اليومية. ولسوء الحظ، كما حدث مع معلوماتنا المالية وبيانات الموقع والبيانات النقالة والاجتماعية، ستتسرب بيانات إنترنت الأشياء الخاصة بنا لتؤمن بذلك إمكانات أكبر وأقوى للمتتبعين والأوغاد الآخرين المهتمين بتعقبنا باستمرار. وبينما سيكون من الممكن بالتأكيد سن قوانين وإنشاء بروتوكولات خصوصية لحماية المستهلكين من أنشطة كهذه، فإن ما يحدث الآن هو مجرد تمهيد لما سيحدث في المستقبل، حيث سيكون الاحتمال الأكبر هو أن كل جهاز مزود بإنترنت الأشياء، سواء كان مكواة أو مكنسة كهربائية أو براداً أو ميزان حرارة أو مصباحاً، سيُرفق مع شروط خدمة، تضمن للمصنعين إمكانية الوصول لكل بياناتك. والأسوأ من ذلك، أنه بينما كان تسجيل الخروج من الفضاء الافتراضي أمراً ممكناً من الناحية النظرية، لن يكون هناك بند للخروج في منزلك الذكي المتصل بإحكام بالشبكة. لذا فإن الكثير مما يحدث وراء الأبواب المغلقة سيكون عرضةً للفحص الدقيق من قبل أطرافٍ لم تقم بدعوتها أبداً إلى منزلك، كما أن إسدال الستائر في هذا العالم لن يحجب شيئاً عن المتلصصين.

قد نجد أنفسنا نتفاعل يومياً مع آلاف الأشياء الصغيرة المحيطة بنا، التي تجمع على مدار الساعة وحدات من البيانات تبدو غير ضارة، وستقوم هذه الأشياء بنقل هذه المعلومات إلى السحابة، حيث ستتم معالجتها وربطها ومراجعتها. وستكشف ساعتك الذكية عدم قيامك بالتمارين الرياضية لشركة التأمين الخاصة بك، وستخبر سيارتك شركة التأمين بمدى سرعتك المعتادة أثناء القيادة، وستقوم حاوية القمامة بإخبار البلدية المحلية بأنك لا تتبع القوانين المحلية لتدوير المهملات. إنه إنترنت المخبرين، وبالرغم من

أنه يبدو بعيد المنال، لكنه يتحقق منذ اليوم. تعرض شركات تأمين السيارات مثل "بروغريسيف" رسوماً مخفضة مصممة بشكل فردي اعتماداً على عاداتك في القيادة. "كلما كانت قيادتك أفضل، ادّخرت أكثر"، كما جاء في الإعلان. فكل ما على السائقين فعله للحصول على سعر أخفض هو الموافقة على تركيب تقنية الصندوق الأسود "بروغريسيف سنابشوت" في سياراتهم، وإتاحة إمكانية تعقب المكابح والتسارع وعدد الأميال بصورة مستمرة. وبينما نمضي قدماً، لا نجاوز المنطق إن اعتقدنا بأن السائقين الذين لا يوافقون على تركيب أجهزة كهذه في سياراتهم سيتحملون أقساطاً فلكية إلى أن تصبح هذه الأجهزة إلزامية بواقع الحال.

سيقدم إنترنت الأشياء قدراً كبيراً من الخيارات للمعلنين تمكنهم من الوصول إليك والاحتكاك معك، من خلال كل جهاز ذكي من أجهزتك الجديدة المتصلة بالإنترنت. وهذا يعني أنك في كل مرة تذهب فيها للبراد لتحضر الثلج، ستقدم إليك إعلانات لمنتجات تتوافق مع الطعام الذي يخمّن برادك أنك تشتريه. ستصبح الشاشات أيضا كلية الوجود، والمسوقون يخططون بالفعل لمجموعة كبيرة من إمكانيات الدعاية. ففي أواخر عام 2013، أرسلت شركة غوغل رسالة لهيئة الأوراق المالية والبورصات تقول فيها "نحن وشركات أخرى سنعرض [قريباً] إعلانات إلى جانب محتوى آخر على البرادات ولوحات عدادات السيارات وموازين الحرارة والنظارات والساعات، وما هذه سوى بعض الاحتمالات فقط". إذا كانت غوغل تقرأ سلفاً حسابك على جيميل، وتسجل كل بحث تقوم به على الشبكة، وتتعقب موقعك المادي على هاتفك المحمول المزود بنظام أندرويد، فأية مفاهيم جديدة ستطورها الشركة عن حياتك الخاصة عندما يكون نظامها الترفيهي موجوداً في سيارتك، وعندما ينظم ميزان الحرارة التابع لها حرارة منزلك، وتراقب ساعتها الذكية نشاطك البدني؟

لن تتعقب تقنية معرفات الهوية الراديوية وغيرها من تقنيات إنترنت الأشياء الأشياء الجامدة وحسب، بل إنها ستستخدم لتعقب الأشياء الحية أيضاً. فقد أصبحت شركات مثل بيت لينك، هوم.أغين، وأي.كي.سي ريونايت شائعة بين محبي الحيوانات المنزلية، فهي تقدم رقاقات معرفات هوية راديوية يمكن زرعها من قبل الأطباء البيطريين، بحيث يمكن تحديد موقع الكلاب والقطط التائهة وإعادتها إلى منزلها إذا هربت. أما ما هو غير معروف إلى هذه الحد على أية حال هو أن الكائنات البشرية بدورها تزداد خضوعاً للمراقبة الإجبارية بوساطة أربطة المعصم المزودة بمعرفات هوية راديوية، كتلك التي باتت شائعة في السجون والمعتقلات من لوس أنجلوس إلى العاصمة واشنطن. حتى إن المسؤولين الحكوميين في بعض البلدان، مثل بريطانيا، ينوون زرع هذه الرقاقات تحت جلد المساجين على غرار الممارسة الشائعة مع الكلاب. وبينما لن يعترض كثير من الناس على تعرض المجرمين للتعقب عبر المعرفات الراديوية، فإن شعور هؤلاء سيختلف عندما يتم تطبيق مثل هذه التقنيات على أطفالهم.

لقد بدأ المسؤولون في المدارس في أنحاء الولايات المتحدة بتضمين رقاقات معرفات هوية راديوية داخل بطاقات الطلاب الشخصية، التي يُطلب من التلاميذ حملها طوال الوقت. وفي مقاطعة كونترا كوستا في كاليفورنيا، يُطلب من الأطفال ممن هم دون سن المدرسة منذ اليوم ارتداء فانيلات تشبه تلك التي يرتديها لاعبو كرة السلة، مزودة بأجهزة تحكم إلكترونية تسمح للمشرفين والمدرسين بمعرفة مكان كل منهم بدقة. وبحسب مسؤولي مدرسة المقاطعة، فإن أنظمة المعرفات الراديوية توفّر "3000 ساعة عمل سنوياً مخصصة لتعقب ومعالجة شؤون الطلاب". بالطبع، عندما يُجبر الناس على الانضمام لإنترنت الأشياء، ستظهر مجموعة كبيرة ومتنوعة من قضايا الخصوصية والسياسات العامة الأخرى. فالمعرفات الراديوية نفسها

التي تتيح مراقبة الطلاب المستمرة على سبيل المثال، ستتمكن من تحديد الطلاب الذين يتحركون "كثيراً"، وستعتبرهم بالتالي مفرطي النشاط ومخربين، وستحكم بأنهم يتلاءمون أفضل مع "مدارس بديلة". أما الطلاب الذين لا يرغبون بأن يتم تعقبهم فسيقال لهم: "حظكم سيئ". وقد تم فصل الطالبة أندريا هيرنانديز في سانت أنطونيو - تكساس عام 2013 عندما رفضت ارتداء جهاز معرف راديوي داخل الحرم الجامعي.

وفي هذه الأثناء، سيصبح من السهل تعقب الموظفين ومعرفة مقدار الوقت الذين يمضونه في تناول الغداء، وطول الاستراحات التي يأخذونها للخروج للحمام وعدد القطع التي ينجزونها. فضلاً عن ذلك، سيتم تسجيل أشياء مثل عدد الكلمات المطبوعة في الدقيقة وحركة العينين وعدد الاتصالات التي تم الرد عليها، وأنماط التنفس والوقت الذي تم إمضاؤه بعيداً من المكتب ومدى الانتباه للتفاصيل. وسيقود ذلك إلى مكان عمل حديث أكثر إنتاجيةً لكنه أشبه بالسجن في الوقت نفسه. وعلى الرغم من ذلك، لن يكون صاحب العمل هو الوحيد القادر على الوصول للبيانات من إنترنت الأشياء لأسباب تتعلق بالكفاءة والتحكم، إذ ستستطيع الحكومة فعل ذلك أيضاً. بل إن أجهزة الشرطة تطلب منذ الآن من المرافق العامة المحلية، أن تكشف عن هوية الزبائن ذوي فواتير الكهرباء العالية بشكل غير معتاد، رابطة الموضوع بزراعة الماريجوانا في الأماكن المغلقة. لقد تم إصدار مذكرات تفتيش واعتقال الزارعين المشتبه بهم، لا لسبب سوى فواتير الكهرباء المرتفعة. وقد يصبح تنفيذ القانون في المستقبل قادراً على الالتفاف على مذكرة الاستدعاء بأن يستعلم عن عدادك الذكي ليتبين ما إذا كان استهلاكك للطاقة "خارجاً عن المألوف" بالمقارنة مع المنازل في حيك.

أما في مسرح الجريمة في المستقبل، فسيكون رجال الشرطة قادرين على استجواب البراد، طارحين عليه شيئاً من قبيل "مرحباً يا صديقي، هل رأيت

أي شيء؟". سيعلم العاملون في مجال رعاية الأطفال أنه لم يكن هناك حليب أو حفاضات في المنزل، وأن الشيء الوحيد الذي كان يحتفظ به البرّاد طوال الأسبوع الماضي هو الجعة. ستتيح إنترنت الأشياء للعالم "السلطة التنفيذية المثالية". فعندما تكون أجهزة الاستشعار مزروعة في كل مكان ويتم تعقب وتسجيل كل البيانات، سيصبح من المرجح أن تتسلم مخالفة مرورية بسبب قيادتك بسرعة ستة وعشرين ميلاً في الساعة في منطقة تبلغ حدود السرعة فيها خمسة وعشرين ميلاً في الساعة، وأن تحصل على مخالفة وقوف بسبب بقائك لسبع عشرة ثانية إضافية مسجلة على عدادك. وكما سبق لكاميرات الضوء الأحمر الحالية أن بينت، عندما يكون كل شيء متصلاً، لا يمكن إخفاء شيء، وخاصة عندما تترجم المخالفات إلى مصدر دخل لأجهزة الحكم وشركائها التجاريين.

أشار المدير السابق لوكالة الاستخبارات المركزية دايفيد بيتريوس، إلى أن إنترنت الأشياء ستكون "نقطة تحول في التجارة السرية". بينما قد يكون النموذج القديم من تجسس الشركات والحكومات قد تورط بإخفاء جهاز تنصت تحت الطاولة في غرفة المؤتمرات بهدف الاستماع لمحادثاتك، سيكون من الممكن الحصول غداً على المعلومات نفسها عن طريق اعتراض البيانات الفورية المرسلة من مصباحك المزود بتقنية وايفاي إلى تطبيق الإنارة على هاتفك الذكي. وبالتالي، قد تكون الأجهزة التي كنت تعتقد أنها تعمل لأجلك في الحقيقة مأجورة من قبل شخص آخر، أي أولئك العاملين في مجال الجريمة.

اختراق الكيان الصلب

قلة قليلة فقط من المخترقين تستهدف العناصر المادية التي يتكون منها نظام الحاسب، كالرقاقات الدقيقة والإلكترونيات وأجهزة التحكم والذواكر والدارات والمكونات والترانزستورات وأجهزة الاستشعار، هذه العناصر التي

تشكل لبّ إنترنت الأشياء. ويهاجم هؤلاء المخترقون البرمجيات الثابتة على الجهاز ومجموعة تعليمات الحاسب الموجودة على كل جهاز إلكتروني نتعامل معه، بما في ذلك أجهزة التلفزة، وأجهزة الاستقبال الصوتية، والهواتف النقالة، ومنصات الألعاب، والكاميرات الرقمية، ومحركات الأقراص الصلبة، والطابعات، والسيارات، وإلكترونيات الطيران، وأنظمة التدفئة والتكييف، والموجهات الشبكية، وأنظمة الإنذار وأنظمة "سكادا" للتحكم الصناعي، ومشغلات يو.إس.بي، والإشارات الضوئية، وعدادات مواقف السيارات، وصمامات محطات الوقود، والساعات الرقمية، وأجهزة الاستشعار، وأنظمة إدارة المنازل الذكية، والروبوتات، وأدوات التحكم المنطقية القابلة للبرمجة (مثل تلك المستخدمة من قبل الإيرانيين في ناتانز). وهذا العدد الهائل من الأشياء "الذكية" غبي على نحو قاتل، وليس لديه أية قدرة على تحديث البرامج الثابتة المحملة عليه سلفاً.

بالفعل، فإن لدى معظم أجهزة الحاسب الصغيرة المدمجة بإنترنت الأشياء، ومعظم الأجهزة الإلكترونية في حياتنا اليومية، قدرة معالجة وذاكرة محدودتين جداً. وهي قيود تفرض تصميماً ذا مواصفات صارمة جداً، بالكاد تستوعب المهام التي يريد مصممو هذه الأجهزة أن تقوم بها، وتجعلهم يتركون مساحة صغيرة ثمينة لكل ما هو "تافه" كالأمن، والذي غالباً ما يمثل خطوةً مؤجلةً جداً من عملية التصنيع. فمعظم البرمجيات الثابتة تفتقر لآلية تلقائية مشتركة لتحديث نفسها بغرض إصلاح أية مسألة وظيفية أو أمنية يتم تحديدها بعد توزيع الجهاز، ما يعني أن أكثر الأجهزة المتصلة بالإنترنت منذ خمس لعشر سنوات هي أهداف سهلة. لكن بعض الأجهزة الأكثر كلفة، مثل الهواتف الذكية، حظيت ببرمجيات ثابتة قابلة للتحديث يمكنها تحميل تحسينات وتصحيحات الأمان. أما بالنسبة لغالبية الأجهزة الإلكترونية الأخرى، فنادراً ما يقوم المصنعون بتغيير برامج الأجهزة الثابتة

خلال عمرها الإنتاجي، لأن القيام بذلك قد يتطلب تغييراً مادياً للدارات المدمجة على المنتج، الأمر الذي سيكون عائقاً اقتصادياً باهظ الكلفة. ولكن حتى لو كان هاتفك يحمل أحدث نسخة من البرامج الثابتة، ثمة الكثير من المخاطر التي يجب أخذها في الاعتبار.

بينما قد يعلم كثير من مستخدمي أندرويد أو آي.فون أن تحميل التطبيق أو ملف الحاسب الخطأ قد ينقل فيروساً لهواتفهم، فإن قلة قليلة، بل ربما معدومة، تعلم أن اختيارها شاحن الهاتف يمكن أن يؤدي للنتيجة نفسها. فقد قام المخترقون بتصميم فيروس يستهدف الكيان الصلب يتم إدخاله مباشرة ضمن شاحن يو.إس.بي مخترق، ويمكنه استهداف أجهزة آبل. إن مجرد توصيل جهازك في أحد أسلاك الكهرباء الشريرة هو كل ما تحتاج إليه لكي تتعرض للإصابة بالفيروس. فعبر تعديل البرنامج الثابت والإلكترونيات في القابس الصغير البريء الذي نستخدمه لشحن هواتفنا، تمكن المخترقون من تجاوز الاحتياطات الأمنية للهاتف ونقل الفيروس إليه. ولم يظهر أي إنذار على الشاشة، ولم يكن البرنامج الذي يعمل خلسةً مرئياً في أي مكان على لائحة البرامج النشطة. أما في الخلفية، فقام الشاحن الشرير بإنشاء باب خلفي في الجهاز يسمح للمخترقين بإجراء الاتصالات، وقراءة الرسائل النصية، وسرقة المعلومات البنكية، والتقاط كلمات السر للحساب البنكي، وتعقب حركة مستخدمي الجهاز. تعرف هذه الظاهرة باسم "جوس جاكينغ"، ولم تتجاوز تكلفة الشاحن الخبيث الخمسين دولاراً. عليك إذاً التفكير في ذلك عندما تصل هاتفك الذكي بعد أن تضورت بطاريته لتشحنه في كشك محطة عامة أو في مطار أو فندق أو مجمع تجاري محلي (وهذه تحديداً هي الأماكن التي قد يضع فيها المخترقون هذه الأجهزة لإصابة أكبر عدد من الضحايا).

ليست الشواحن المعدلة بصورة غير شرعية هي الأجهزة الوحيدة التي

تخبئ لنا المفاجآت ويجب أن نحذر منها اليوم، بل ينطبق ذلك على كل شيء مزود بجهاز تحكم دقيق أو جهاز استشعار يمكن أن يصل لمنزلك مع "مواصفات متقدمة" لن يرغب بها أحد. ففي عام 2013 لاحظ مسؤولو الجمارك في روسيا أن مجموعة من البضائع الاستهلاكية المصنعة في الصين، ومن ضمنها أجهزة إلكترونية كغلايات الشاي، ومكاوي الملابس، وصلت مع تعديلات لم تكن السلطات الروسية مسرورة بها كل السرور. إذ كانت الأجهزة تحتوي على بطاقات وايفاي مصغّرة قادرة على نشر البرامج الخبيثة على أي شبكة إنترنت مفتوحة ضمن نطاق مئتي متر، كما كانت قادرة على "الاتصال بالوطن"، ونقل رسائل سرية إلى الصين. ليست غلايات الشاي والمكاوي قادرة على الانضمام خلسة إلى شبكة الوايفاي الخاصة بك فحسب (وهذا شيء لا يمكن لأحد أن يتوقعه من مكواة عادية يستخدمها يومياً)، بل يمكنها أيضاً أن تستخدم شبكة الإنترنت الخاصة بك لنشر الفيروسات على أجهزة حاسب أخرى موجودة في منزلك، ونشر رسائل بريد مزعجة لجيرانك وباقي العالم. وبينما يحلو لنا أن نصدق أن المكاوي الجاسوسة وشواحن هواتف الآيفون المخترقة ليست إلا مجرد حوادث غريبة، فإن حقيقة الأمر هي إنها ليست سوى نذير بتهديدات أخرى أكثر جدية وانتشاراً بسبب الاستيعاب السريع لبلايين الأجهزة المتصلة بالشبكة في شبكة المعلومات العالمية.

المزيد من الاتصالات، المزيد من نقاط الضعف

مقابل جميع منافع إنترنت الأشياء التي لا يمكن حصرها، قد تكون لها مساوئ هائلة. فإضافة 50 بليون شيء جديد لشبكة المعلومات العالمية بحلول عام 2020، يعني أن كلاً من هذه الأجهزة سيكون قادراً على التفاعل مع الأشياء الأخرى المتصلة الموجودة على كوكب الأرض، والتي يبلغ عددها 50 بليوناً، سواء كان هذا الاتصال بقصد الخير أم الشر. وستكون النتيجة 2.5

سيكستليون تفاعلاً محتملاً بين شيء متصل وشيء آخر، وهي شبكة واسعة جداً ومعقدة يصعب فهمها أو نمذجتها. ستصبح إنترنت الأشياء شبكة عالمية لها تبعاتها ومفاجآتها غير المتوقعة حين تقوم بأشياء لم يصممها أحد ولم يقم أحد بالتخطيط لها عن قصد. قد تكون هناك فوائد سيتم اكتشافها بالصدفة لمثل هذه الشبكة، لكن ثمة أيضاً فرصة كبيرة لأن تكون العديد من تطويراتها غير مستحبة وأن يكون لها تأثير سلبي على الأمن العالمي، والخصوصية الشخصية، وحقوق الإنسان. علاوة على ذلك، إن كنت تعتقد أن عدد رسائل الأخطاء وأعطال التطبيقات التي نواجهها اليوم مشكلة، فانتظر فقط حتى تصبح الشبكة مدمجة في كل شيء، بدءاً من سيارتك وحذائك الرياضي وصولاً إلى الميكروويف في مطبخك. إذ لن يكون من المسلي أن تضطر لإعادة تشغيل البراد وميزان الحرارة وباب المرآب لكي تعود هذه الأشياء للعمل.

إذا كانت هناك تقنية قادرة على تجسيد أثر الفراشة، فهي بالتأكيد تقنية إنترنت الأشياء. ففي هذا العالم، من المستحيل معرفة العواقب التي ستنتج عن وصل خلاط المنزل المتصل بالإنترنت لنفس شبكة المعلومات التي تتصل بها سيارة إسعاف في طوكيو، وجسر في سيدني، وخط إنتاج لتصنيع السيارات في ديترويت، وستكون كلها متصلة في ما بينها بالفعل بطريقة أو بأخرى.

بينما تسارع بعض شركات التكنولوجيا والأبحاث الأذكى في العالم لإنشاء إنترنت الأشياء (وتطالب بحصتها من عوائده الاقتصادية التي تقدر بالعديد من تريليونات الدولارات)، ينكب العاملون في أقسام أمن تكنولوجيا المعلومات في الخلفية، على العمل بشكل محموم لمواجهة هجمات اليوم صفر التي كانت تُشَن بالأمس، أو أزمة نقاط الضعف الكامنة التي تكشفها البرامج الخبيثة اليوم. وليس هناك الكثير من الوقت للتكهن أو التحضير لما

سيأتي لاحقاً. فالمستويات الهائلة للجرائم الافتراضية التي نواجهها اليوم تؤكد بما لا يدع مجالاً للشك أننا لن نستطيع حماية أجهزة الحاسب المكتبية والمحمولة الشائعة المتصلة بالإنترنت في الوقت الحاضر، ناهيك بمئات ملايين الهواتف النقالة والأجهزة اللوحية التي نضيفها سنوياً. فضمن أية رؤية مستقبلية يمكننا إذاً أن نتصور قدرتنا على حماية الخمسين بليون شيئ التي ستتصل بالإنترنت لاحقاً؟ ومع عدم قدرتنا على ضمان أمن شبكة المعلومات العالمية اليوم، فكيف سنتمكن من حماية عالم كل شيء مادي فيه متصل بالشبكة وقابل للاختراق من أي مكان على كوكب الأرض، بدءاً من الحيوانات الأليفة وصولاً لأجهزة ضبط نبضات القلب والسيارات الذاتية القيادة؟ إن الواقع الساطعة يقول إننا لا نستطيع.

لن تكون إنترنت الأشياء أكثر من إنترنت أشياء قابلة للاختراق، أو كماً كبيراً من الفرص الخبيثة تتاح لأولئك الذين يملكون الوسائل والحافز لاستغلال غياب الأمان التقاني الشائع لدينا. وستفتح إنترنت الأشياء والبروتوكولات غير الآمنة التابعة لها صندوق باندورا المليء بنقاط الضعف الأمنية غير المسبوق، بل إنها ربما تؤدي إلى أعطال وظيفية في الأنظمة سيكون مداها مبهراً ومرعباً وغير متوقع في آنٍ معاً.

هيوستن، لدينا مشكلة، ألا وهي اتساع نطاق التهديد، أي في عدد النقاط أو مصفوفات الهجوم التي يمكن للعدو أن يضرب من خلالها. إن التحدي الكامن في إنترنت الأشياء هو أن نطاق التهديد التقني يزداد اتساعاً على نحو أسي. وإذا أردنا أن نبسط الأمور، فإنه ليس لدينا أية فكرة عن كيفية الدفاع عن هذا النظام بشكل فعال. والمنطق واضح: كلما كان لديك نوافذ وأبواب، ازدادت قدرة اللص على الدخول لمنزلك، وخاصة إذا كان متصلاً بالإنترنت.

الفصل الثالث عشر
بيتي السعيد، بيتي المُخترق

تبين تقديراتنا أن واحداً بالمئة فقط من الأشياء التي يمكن أن تملك عنوان إنترنت قد زوّدت بالفعل بمثل هذا العنوان، لذا يسعدنا أن نقول إن تسعةً وتسعين بالمئة من العالم لا يزال نائماً. ونترك لمخيلاتنا أمر ما سيحدث عندما تستيقظ التسعة والتسعون بالمئة الباقية.

بادماسري واريور، رئيس قسم التكنولوجيا، سيسكو

لم يكن بليك روبينز، الطالب في مديرية مدرسية لور ميريون في بنسلفانيا، قادراً على أن يتخيل السبب وراء استدعائه لمكتب المدير. فعندما اتهمت مساعدة المدير الطالب البالغ من العمر ست عشرة سنة بالقيام بـ "تصرف غير ملائم"، ردّ روبينز بأنه لا علم له إطلاقاً بما تتحدث عنه مسؤولة المدرسة. فأوضحت عندها مساعدة المدير السبب: لقد كانت تعلم بأن الطالب كان يتاجر بالمخدرات وهددته بالفصل من المدرسة. أنكر الشاب هذه الاتهامات بشدة إلى أن التفتت المشرفة إلى حاسبها الشخصي فجأة لتعرض أمام روبينز صورةً له في غرفة نومه وهو يحمل حبوباً مستطيلة الشكل في يده ومن ثم يقوم بابتلاعها. وحين سأل الشاب المصدوم عن مصدر الصور، لم تشعر المشرفة أنها مضطرة للتفكير في الأمر.

عاد روبينز إلى منزله ليقص ما حدث على والديه اللذين واجها مديرية المدارس بالمسألة. وكما تبيّن لاحقاً، لم يكن روبينز يتعاطى المخدرات أو يتاجر بها، بل كان يتناول "حلوى ميكي أند إيكي" فقط، وهي حقيقة يعرفها والداه. لكن كيف تمكّن مسؤولو المدرسة من تصوير الشاب البالغ من العمر ست عشرة سنة في غرفة نومه وهو يتناول الحلوى؟ عبر برنامج تجسس دقيق يزعمون أن هدفه حماية حرمة المدرسة.

لقد قام مسؤولو مديرية المدارس الميسورة بتزويد ألفين وثلاثمئة طالب

ثانوية بحواسب ماك.بوك لمساعدتهم في دراستهم. لكن ما لم يكشفه المسؤولون للطلاب والأهالي على حد سواء، هو أن أجهزة الحاسب هذه مزودة ببرنامج سري يؤمن لمشرفي المدرسة إمكانية الوصول عن بعد لجميع نشاطات الطلاب التي يقومون بها على هذه الأجهزة، بما في ذلك سجلات الدردشة بين الطلاب وبيانات بالمواقع الإلكترونية التي قاموا بزيارتها. كما يسمح هذا البرنامج للمسؤولين بتجنيد كاميرا جهاز الحاسب الشخصي عن بعد لتصوير وتسجيل حركة الطلاب في أي وقت ما دامت أجهزة الحاسب هذه مفتوحة، كل هذا للمساعدة في تعقب الأجهزة الضائعة أو المسروقة حسب زعمهم. وقد تم إعداد نظام التجسس عن بعد هذا بحيث يلتقط صوراً بشكلٍ صامت كل خمس عشرة دقيقة عندما يكون جهاز الحاسب في وضع التشغيل، ولو أنه يمكن للمسؤولين أن يحددوا الفواصل الزمنية بين الصورة والتي تليها لتصل إلى ستين ثانية للطلاب الذين يشتبه بقيامهم بـ "تصرفات غير ملائمة".

يتم رفع الصور الملتقطة على مخدّم الشبكة الخاص بمديرية المدارس، حيث تتم مراجعتها بشكل فردي من قبل مسؤولي المديرية. وقد التقط مسؤولو المقاطعة أكثر من ستٍ وخمسين صورة، من ضمنها صورٌ لأطفالٍ عراة في غرف النوم وفي الحمامات وفي أي مكان ذهب إليه الأطفال برفقة حواسبهم المحمولة. وجمع المشرفون خلسةً ما يفوق الأربعمئة صورة لروبينز وحده عندما اشتُبه بقيامه بأفعال سيئة، دون أن يتم إعلام الشرطة أو إصدار مذكرات تفتيش نتيجة تصرفات مديرية المدارس التدخلية. ولكن ما إن انتشرت الأخبار عن التصرف الفاضح لمديرية المدارس، رفع العديد من الدعاوى القضائية، وكان من بينها الدعوى التي رفعها أهل روبينز. وتبع ذلك تحقيقٌ جنائي أجراه مكتب التحقيقات الفيدرالي بحق المديرية. وكما أخبر روبينز برنامج "صباح الخير أميركا"، "الأمر أشبه بأن يجلسوا في

غرفتي ويتفرجوا عليّ دون علمي". لكن لسوء حظ طالب السنة الثانية، فإنه كان صغيراً جداً على دراسة النبوءة التي تحذر من الإغريقيين المحمّلين بالهدايا، فهو موضوع سيدرسه على الأرجح بعد سنتين عندما تُطلب منه دراسة قصيدة الإنياذة للشاعر فرجيل ضمن دروس اللغة الإنكليزية المتقدمة.

الكاميرا الخفية

لا يمكنك أن تزعم بأن أي مكان تذهب إليه هو مكانٌ خاص نظراً لما وصلت إليه وسائل المراقبة من وفرة وقابلية للتخفّي.
هاورد راينغولد

عندما تمتلك مديرية مدرسية حكومية، وهي مكون من مكونات الدولة، إمكانية التجسس علينا في منازلنا كما تشاء وبدون مذكرة أو تصريح، فمن الواضح أن عصر المراقبة الشاملة المتغلغلة قادمٌ إلينا. لقد تم تركيب شبكات المراقبة الضخمة، المعروفة باسم دوائر التلفزة المغلقة أو سي.سي.تي.في، من لندن إلى نيويورك ومن شيكاغو إلى بكين لحمايتنا من التهديدات الحقيقية والمتخيلة. بل إن المسؤولين في مدينة واحدة هي مدينة تشونغكينغ جنوب غرب الصين، قاموا بتركيب 500,000 كاميرا للتعامل مع الاضطرابات السياسية والدينية إلى جانب "جرائم منظمة" أخرى. وإذا كانت الحكومة هي من كان يتحكم بمثل هذه الأنظمة الأمنية ذات يوم، فإننا اليوم غالباً ما نواجه الكاميرات في محالّ البقالة ومحطات الوقود ووكالات السيارات والمستشفيات ومباني المكاتب والجسور والأنفاق، والبارات وسيارات الأجرة والباصات والقطارات وعيادات الأطباء ومحالّ تنظيف الملابس. وهي موجودة أيضاً على حواسبنا المحمولة وهواتفنا النقالة وكاميرات مراقبة مربيات الأطفال وأنظمة الأمان في المنازل. وكلما

انتشرت هذه الأجهزة، قل إدراكنا لوجودها أصلاً. ونظراً للكلفة شبه المعدومة لأجهزة تحليل وتسجيل الفيديو، فإن وجودها سيتوسع توسعاً كبيراً في حياتنا مع تطوير مفهوم جديد للمراقبة خاص بالإنترنت.

يجري تحسين نوعية وإمكانات كاميرات اليوم وصولاً إلى مستويات لا يمكن تصورها، مقارنة بالصور المشوشة بالأبيض والأسود التي كانت مستخدمة في الماضي. وقد وزّعت وزارة الدفاع بالفعل كاميرا بدقة 1.8 غيغا بيكسل يمكن وصلها بطائرة مسيّرة ويمكنها أن ترصد الأهداف "بحجم يصل إلى 6 بوصات من ارتفاع يعادل 20,000 قدم". (ولا شك في أن هذه التقنية ستصبح متوفرة تجارياً في المستقبل القريب). علاوة على ذلك، لا تقوم كاميرات اليوم بالمراقبة والتسجيل فقط، بل يمكنها أن ترى وتفهم أيضاً عبر ربط أجهزة الاستشعار الخاصة بها بخوارزميات الحوسبة السحابية وتحليل البيانات الكبيرة. ونتيجة لذلك، يمكن للكاميرات أن تتعرف وجهك وأن تقرأ رقم لوحة سيارتك، بل وأن تحدد ما إذا كان طردٌ ما (قنبلة محتملة) قد تُرك في مكان لفترة أطول من اللازم. ويمكن إجراء هذا التحليل بالزمن الحقيقي وبأثرٍ رجعي، ما يجعل فتح ملايين الساعات من تسجيلات الفيديو لأوقاتٍ سابقة للبحث عن "امرأة ترتدي قبعة حمراء" أمراً ممكناً.

لسوء الحظ، يمكن للأدوات المصممة بغرض حمايتنا أن تعطينا إحساساً زائفاً بالأمان، وقد أثبتت مئات ملايين الكاميرات المتصلة بالإنترنت حول العالم ضعفها أمام هجمات المخترقين ونواياهم السيئة. وكما ناقشنا آنفاً، يمكن تشغيل كاميرا هاتفك المحمول عن بعد بسهولة وبدون معرفتك باستخدام أدوات منتشرة بكثرة، مثل موبايل سباي (الذي بيعت منه ستون ألف نسخة).

من الشابات اللواتي لُقّنَّ هذا الدرس بطريقةٍ قاسية كاسيدي ولف، ملكة جمال مراهقات أميركا. فقد تم التحكم بكاميرا حاسبها المحمول من قبل

أحد المخترقين، فراح يلتقط لها صوراً ومقاطع فيديو وهي تتجول في غرفة نومها عارية بعد خروجها من الحمام أو بينما كانت ترتدي ثيابها للذهاب إلى المدرسة. وكان المتحرش يشاهدها يومياً على مدى عدة أشهر، إلى أن أرسل لها في أحد الأيام بريداً إلكترونياً يبتزها فيه جنسياً ويطلب منها القيام بمجموعة من الأفعال الجنسية أمام الكاميرا لأجله، "أو سأقوم برفع هذه الصور والكثير غيرها (لدي الكثير من الصور وبجودة أعلى) ونشرها على كل حساباتك ليراها كل الناس. وبهذا لن تحلمي بأن تصبحي عارضة أزياء بل نجمة أفلام إباحية [إلخ]". عقب تسلمها رسالة التهديد الإلكترونية، أغلقت كاسيدي جهاز الحاسب بعنف وانفجرت باكية، لتقرر في النهاية الذهاب إلى الشرطة. وبعد مرور ثلاثة أشهر، كشف تحقيق قام به مكتب التحقيقات الفيدرالي أن أحد زملائها في المدرسة، ويدعى جارد أبراهام، هو من كان يبتزها. وقد نفّذ أبراهام هجومه مستعيناً بـ بلاك شيدز، وهي مجموعة أدوات توفّرها شركة الجريمة يمكن شراؤها بسهولة من مواقع الجريمازون، كما استخدم البرمجية الخبيثة لاستهداف ثماني نساء أخريات في جنوب كاليفورنيا.

أصبحت كاميرات مراقبة الأطفال الحديثة اليوم، والتي تسمح للأهل بمراقبة الأطفال ليس فقط في الغرفة المجاورة بل عبر الإنترنت، تمثّل منفذاً جديداً على الشبكة ينتظر أن يتم اختراقه. وقد قام المخترقون والمتحرشون بالأطفال مراراً باختراق هذه الأجهزة، حيث لا تحتاج الغالبية العظمى منها لكلمة سر أو أنها تستخدم كلمة سر افتراضية معروفة تضعها الشركة المصنعة، ما أدى في النهاية إلى نشوء تجارة مزدهرة لصور كاميرات مراقبة مربيات الأطفال في الأوساط الرقمية السرية، ومن ضمنها صور لأمهات شابات يرضعن أطفالهن من صدورهن. وتسمح الكاميرات بزاوية رؤية كاملة وبإمالة الصورة وتكبيرها، كما أنها تتضمن نظام صوت ثنائي المسار

مع ميكروفون وسماعات مصممة داخلها، بحيث يتمكن الأهل من الاستماع لأطفالهم والتحدث إليهم، وهي ميزات ملائمة ومريحة للأم والأب وللمخترق على حدٍّ سواء، كما اكتشفت هيذر شريك من سنسناتي عندما تم إيقاظها من نومها العميق في منتصف الليل.

"فجأة، سمعت ما بدا لي كأنه صوت رجل، لكنني كنت نائمة، لذا لم أكن متأكدة". قامت هيذر وهي مضطربة بالتحقق باستخدام هاتفها المحمول من كاميرا الطفل في غرفة نوم طفلتها إيما البالغة من العمر عشرة أشهر. كانت الكاميرا تتحرك بشكل غريب، لكن لم تكن الأم هي من يحركها. وفجأة سمعت هيذر صوت رجل في منزلها يصرخ "استيقظ أيها الطفل، استيقظ!". ركضت هيذر مع زوجها آدم إلى غرفة نوم إيما، وعند دخولهما تحولت كاميرا المراقبة عن طفلتهم الباكية لتركز على آدم. وأطلق الصوت الذكوري القادم عبر الجهاز الموجه نحو الأهل العنان لخطبة عصماء من الشتائم على الزوجين اللذين لم يكونا قد استيقظا تماماً بعد، إلى أن أسعف آدم الموقف بنزع سلك الكاميرا بهدوء من الحائط. واعترفت الشركة المصنعة لجهاز مراقبة الطفل "فورسكام" لاحقاً بأن "الجهاز كان يحتوى على ثغرات في برمجياته الثابتة"، سمحت بالتسلل إلى مهد طفلة آل "شريك" النائمة. ليست هذه الحوادث فردية إطلاقاً، كما اكتشفت عائلة أخرى في هيوستن عندما استيقظت على صوت رجلٍ يصرخ باسم طفلتهم "أليسون" البالغة من العمر سنتين، موجهاً لها الشتائم وهو ينتحب، "استيقظي... أيتها العاهرة الصغيرة". كان الدخيل الافتراضي يعلم اسم الطفلة لأنه كان مكتوباً باللون الزهري على الحائط. إنه لأمرٌ مثيرٌ للسخرية والغضب بآنٍ واحد أن هذه الأجهزة التي تشتريها العائلات لحماية أنفسها يمكن استخدامها في الحقيقة كأسلحة تشرع ضدها وكأنها تستدعي المشاكل إلى منزلها.

إضافةً إلى كاميرات مراقبة الأطفال، تعاني الكاميرات الأمنية في المكاتب والمنازل نقاط الضعف نفسها، وقد اكتشف الباحثون عيوباً منتشرة بشكلٍ واسع في أكثر من عشرين ماركة كبرى، تم بيع معظمها مزودةً بإمكانية الوصول للإنترنت عن بعد مع إعدادات أمنية افتراضية ضعيفة. ولا يقوم ما يقارب 70 بالمئة من المستخدمين بتغيير اسم المستخدم الافتراضي، مثل "يوزر" أو "أدمِن"، كما أنهم لا يغيرون كلمة السر الموضوعة مسبقاً من قبل الشركة المصنعة، والتي عادة ما تكون شيئاً مثل "1111" أو "1234". نتيجة لذلك، تصبح عشرات ملايين الكاميرات المتصلة بالإنترنت مفتوحة على مصراعيها جاهزة للاعتراض من قبل جهاتٍ مجهولة، وسيكون المخترقون سعداء بمشاركة اكتشافاتهم التلصصية. فمن دون موافقة أو معرفة الناس الذين تتم مراقبتهم، تتوفر على الإنترنت الآلاف من مثل هذه اللقطات المباشرة، ويمكن لأي شخص أن يشاهدها: خدمة غسيل آلي في لوس أنجلوس، أو رجل في نيويورك يشاهد مباراة كرة القدم على أريكته، أو زبائن في أحد البارات في فرجينيا، أو غرفة معيشة في هونغ كونغ، أو مكتب في موسكو، اختر ما تشاء. ونظراً للفرص المتاحة، لم يمض وقتٌ طويل حتى بدأت شركة الجريمة باستكشاف أفضل الطرق التي تسمح لها باستغلال الكاميرات المزودة بنظام إنترنت الأشياء.

لم لا نخترق كاميرا البنك قبل أن نسرقه، لمعرفة نمط سلوك الموظفين وموعد وصول شحنات النقد وأوقات استراحة الحراس؟ نحن نعلم بالطبع أن معظم سرقات البنوك لا تحقق إلا مبلغاً تافهاً مع خطورة عالية، لكن ثمة أسماك أكبر يمكن قليها. هذا بالضبط ما قام به فريقٌ من المجرمين من شركة الجريمة في آذار عام 2013، عندما نفذوا هجوماً على طريقة فلم "أوشينز إيليفن" على كازينو كراون في مدينة ملبورن في أستراليا. حيث استولى المخترقون على نظام الأمن الخاص بالكازينو واستخدموا كاميرات المنتجع

الأمنية للتجسس على المبنى، بما في ذلك غرف القمار الخاصة بكبار الزوار. وكان المشتبه به الأول، والذي وُصف على أنه أجنبيٌّ، يُعرف باسم "الحوت" فقط، مقامراً كبيراً كان يراهن بانتظام على مبالغ كبيرة من المال، باستثناء هذه المرة التي كان لديه فيها ميزة إضافية. فبعد اختراقه مع شركائه للبث المباشر للفيديو، باتوا قادرين على رؤية كل أوراق اللعب التي بيد الموزع وأقرانه اللاعبين على طاولة البوكر التي كان يجلس عليها. وبينما كان الحوت المجرم يتهادى في طريقه للعب مع كبار المقامرين، كان زملاؤه المخترقون المختبئون يزودونه بتعليمات المراهنة عبر سماعة لاسلكية مخفية. واستطاع المخترق الواثق من رهانه أن يربح أكثر من 33 مليون دولار أميركي خلال ثماني جولاتٍ فقط. وبدلاً من المخاطرة، غادر الرجل المكان ثرياً وعاد إلى بلده قبل أن تلاحظ السلطات ما حصل. بينما تمضي الخطى بسرعة هائلة نحو إنترنت الأشياء، سيكتشف المزيد من الناس أن الأشياء التي وثقوا بها وتوقعوا منها أن تحميهم، سواء كانت الكاميرات الأمنية أو أكياس الهواء، يمكن استغلالها من قبل الآخرين واستخدامها ضدهم بطرق مفاجئة، بل قاتلة.

من سرقة السيارات إلى اختراقها

> يفضّل معظم الناس أن ترتع البرمجيات الخبيثة في حواسبهم المحمولة بدلاً من أن تصيب نظام مكابح السيارة.
>
> البروفسور كريستوف بار، باحث في مجال الأمن المدمج

كانت السيارات تعمل بالغازولين ذات يوم، لكنها صارت اليوم تعمل بالشيفرات البرمجية. ولا تزال بحاجة للغازولين أو الكهرباء للطاقة، ولكن بدون شيفرة حاسوبية فعالة، ستتوقف أية سيارة حديثة عن العمل في منتصف الطريق. وإذا كانت سيارة والدك من طراز شيفروليه 1957 تعتبر جهازاً ميكانيكياً بحتاً، فإن سيارات اليوم ليست إلا أجهزة حاسب على

عجلات. إذ تملك السيارة التي تدلف من خط الإنتاج في عام 2015، ما بين سبعين إلى مئة جهاز حاسب على متنها تعرف كل منها باسم وحدات التحكم الإلكترونية. تدير هذه الوحدات مع بعضها محرك السيارة وجهاز التحكم بالسرعة ونظام منع انغلاق المكابح والتكييف والنقل والترفيه، ومسّاحات الزجاج الأمامي والمقاعد الكهربائية والأقفال ونظام الملاحة وكفاءة استهلاك الوقود وأكياس الهواء، على سبيل المثال لا الحصر. ورغم قيام صانعي السيارات بعمل جيد حين جعلوا كل هذه الأجهزة غير مرئية، فإن سيارات اليوم تمثل نظاماً شديد التعقيد يحتوي على ما يقارب 100 مليون سطر من الشيفرة الحاسوبية (مقابل رقم ضئيل نسبياً هو 1.7 مليون سطر هو عدد سطور الشيفرة البرمجية التي تدير إلكترونيات الطيران على الطائرة الحربية الأميركية "إف 22"، المصممة للقتال على الخطوط الأمامية). تشكّل كل هذه الإلكترونيات المدمجة نحو 50% وسطياً من كلفة السيارة الجديدة (ونحو 80% في السيارات الهجينة). وتشكّل هذه الرقاقات الدقيقة شبكة منطقة المتحكمات، أو "كان"، وهي شبكة الحاسب الموجودة على متن السيارة التي تمثل شريان الحياة لأي سيارة حديثة، كما أنها مسؤولة عن تحسين مستوى الأمان وخفض كمية الانبعاثات وزيادة معدل الأميال في سياراتنا أكثر من أي وقت في التاريخ.

لا تتواصل هذه التقنيات المدمجة في ما بينها عبر شبكات "كان" وحسب، بل إنها تشارك المعلومات على نحو متزايد مع العالم الخارجي عبر مجموعة متنوعة من شبكات الراديو والشبكات الخلوية الموجودة داخل السيارة نفسها، ما يوفر قدراً كبيراً من الراحة للسائقين. إذ تتيح شبكة "بي.إم.دبليو تيلي سيرفس" للحساسات الداخلية في السيارة إجراء عملية تشخيص ذاتي مستمرة، وإرسال تقارير بالأعطال للوكيل المحلي. وعندما يتم الكشف عن مشكلةٍ ما، يتلقى مالك السيارة اتصالاً لإخباره بأن سيارته معطلة وأنه

يمكنه المجيء لترتيب موعد لفحصها. سيتصل نظام أُن.ستار من شركة جي. إم تلقائياً بسيارة إسعاف إذا كشفت وسادات الهواء وحساسات الحركة تعرّض إحدى السيارات لحادث.

بينما يمكن للصناديق السوداء التي تسجل بيانات الأحداث أن تساعد في خفض قيمة أقساط التأمين، يمكنها أيضاً أن تستعلم عن كل حركة تقوم بها، لتولّد بالتالي مئات الميغابايتات من البيانات في الثانية. وتتعقب هذه الأجهزة عدداً هائلاً من المؤشرات المركبية، مثل الموقع واستخدام حزام الأمان والسرعة وتشغيل إشارات الانعطاف. وقد اعترف جيم فارلي، نائب الرئيس للتسويق والمبيعات العالمية لشركة "فورد موتورز"، في بداية عام 2014، "[نحن نعرف] كل شخص يخترق القانون، ونعرف متى يتم ذلك. لقد وضعنا نظام تحديد المواقع العالمي في سيارتك، لذا نحن نعلم ماذا تفعل". والأمر لا يقتصر على شركة "فورد" وحسب، فقد سبب نظام أون.ستار لشركة جي.إم غضباً عارماً عندما قامت بتحديث شروط الخدمة في خطوة أحادية الجانب لتضمن لنفسها حقاً أبدياً بمراقبة جميع سياراتها، بما في ذلك قراءة الموقع وعداد المسافة، ومشاركة هذه المعلومات مع أطرافٍ أخرى، حتى بعد إنهاء الخدمة من قبل مالك السيارة. أوه، وذلك الميكروفون المريح المصمم داخل السيارة الذي يسمح لك بسؤال أون.ستار عن الاتجاهات ويستمع إليك بعد حصول اصطدام، يمكن أيضا تشغيله عن بعد بدون علمك للإصغاء إلى محادثاتك الخاصة، وهذا ما يقوم به مكتب التحقيقات الفيدرالي منذ عام 2003 على الأقل في إطار التحقيقات المتعلقة بالغوغاء.

قد تكون هناك مخاوف متعلقة بمستقبل سيارتك أكبر من قضية الخصوصية وحدها. فالتعقيد المتزايد في السيارات الحديثة يقود إلى عمليات استدعاء للسيارات، بسبب أعطال في النظام وإلى خسائر بشرية

فادحة. فخلال الأشهر الستة الأولى من عام 2014 فقط، أُجبرت "جي.إم" على استدعاء 29 مليون سيارة، وأكثر منها بملايين لشركة نيسان وهيونداي وفورد وهوندا وبي.إم.دبليو. فعندما تتحكم الإلكترونيات الشديدة التعقيد الموجودة في السيارة بكافة وظائفها الرئيسية، قد يصبح لأعطال النظام آثار غير متوقعة، كسلسلة المشاكل التي تعرضت لها شركة "تويوتا" في أواخر العقد الأول من القرن الحادي والعشرين وأدت إلى موت سبعة وثلاثين سائقاً. فقد وجدت المحكمة أن العديد من الاصطدامات قد تعود إلى عيوب في برامج نظام التحكم الإلكتروني بالكابح، تتسبب ببقاء الضغط على دواسة الوقود وفشل مكابح السيارة. وقد تم اتهام "تويوتا" بالتستر على العيوب، وتم التوافق عام 2014 على دفع غرامة 1.2 مليار دولار لوزارة العدل الأميركية لتقديم "تويوتا" الربح على السلامة. وما حوادث السلامة العرضية هذه سوى جزء من المشكلة بالطبع. فعندما تصبح السيارات أجهزة حاسب تغدو، كغيرها من الأنظمة، أهدافاً جذابة للمخترقين الخبثاء.

لقد أصبحت الأيام التي كان يستخدم فيها السارقون علاّقات الملابس لسرقة السيارات جزءاً من الماضي. كما لم تعد هناك حاجة لإشهار مسدسٍ في وجه أحدهم لسرقة سيارة؛ فقد دخلت سرقة السيارات العصر الحديث الذي يتم فيه اختراق السيارة اختراقاً. يفرض على كافة السيارات التي يتم تصنيعها منذ عام 1996 في الولايات المتحدة وضع منافذ إلكترونية تشخيصية موحّدة على متنها، لتؤمن وصولاً مادياً مباشراً لأنظمة الحاسب المركزية في العربة، كما أن مجموعة كبيرة من بروتوكولات الاتصال مثل المعرف الترددي الراديوي، أو آر.إف.آي.دي، والبلوتوث والاتصالات النقالة تؤمن مثل هذا الوصول عن بعد. حتى إن السيارات الأحدث أصبحت مزودة بمنافذ يو.إس.بي. وكالعادة، فإن المزيد من الاتصالات يعني مزيداً من نقاط الضعف. فوفقاً لمجلة "لندن ميتروبوليتان بوليس"، فإن نحو

نصف السيارات التي سُرقت في لندن عام 2013، والبالغ عددها تسعة وثمانين ألفاً، قد تم اختراقها من قبل مجرمين يستخدمون مجموعة متنوعة من الأجهزة الإلكترونية لفتح وتشغيل السيارات. ويمكن شراء أدوات السرقة المستخدمة في تلك الهجمات من مواقع جريمازون، حيث يقدمها مزودون من بلغاريا في الغالب. ولا يستغرق إنجاز العملية أكثر من عشر ثوانٍ. وبالطبع فثمة فيديوهات على مواقع جامعة الجريمة توضح العملية بأكملها.

يمكن للصوص برمجة مفتاح إلكتروني فارغ، ليحل محل مفتاح السيارة الأصلي باستخدام أدوات بحجم الهاتف النقال يستخدمها في الأصل صانعو الأقفال لمساعدة الأفراد الذين فقدوا مفتاح سيارتهم الإلكتروني. وتوهِم تقنية انتحال الهوية هذه السيارة بوجود سلسلة المفاتيح الأصلية الخاصة بالمالك، ويمكن إنجاز العملية إما عن طريق الاعتراض اللاسلكي لإشارات الراديو التي تستخدمها عندما تفتح أو تقفل سيارتك، أو عبر استهداف حاسب السيارة مباشرةً.

يمكن للصوص فتح باب سيارتك والانطلاق بها باستخدام حاسب محمول ورسالة نصية تتضمن التعليمات المشفّرة الصحيحة فقط لا أكثر. وقد تعرضك ذائقتك الموسيقية للخطر أيضاً كما أثبت عددٌ من الباحثين في المجال الأمني عام 2011، عندما حقنوا شيفرة حاسوبية خبيثة في ملفٍ موسيقي من نوع إم.بي.ثري وقاموا بنسخ مجموعة من الأغاني على قرصٍ مضغوط. وعند تشغيل القرص باستخدام نظام الصوت في السيارة، يقوم الملف الموسيقي المصاب بتشويه البرمجيات الثابتة في المركبة، ما سمح للمخترقين بالوصول لكافة أنظمة التحكم الرئيسة فيها. في حالةٍ كهذه، قد تكون سرقة السيارة أفضل الاحتمالات، إذ لا يمكن حصر الاحتمالات الواردة عندما يتم اختراق نظام القيادة في السيارة.

بأقل من 30 دولاراً، يمكن للمخترقين أن يصمّموا جهازاً مثل جهاز "كان هاكينغ تول"، والذي يسمح للمخترقين بمجرد وصله بالشبكة الحاسوبية للسيارة بأن يتحكموا بالأضواء والأقفال والمقود والمكابح في مركبتك. وبما أن كل عنصر من عناصر سيارتك تقريباً يتم التحكم به عن طريق نظام حاسوبي، فإن وجود أجهزة كهذه يعني إمكان الوصول إلى أي سيارة وهي تسير ولمسها من الطرف الآخر من العالم عبر تخريب مستقبلات الهاتف النقال المدمجة في السيارة نفسها. أما عن مسافة أقرب، فيمكن اختراقها عن طريق "البلوتوث" أو الـ "واي فاي". وقد أثبتت عشرات البراهين التي قدمها مخترقون وباحثون في المجال الأمني، أنه من الممكن جداً أن يسيطر مجرمون عن بعد ألفٍ وخمسمئة ميلٍ على سيارتك خلال قيادتك لها على الطريق السريع بسرعة خمسة وستين ميلاً في الساعة. أما ما قد يفعلونه بسيارتك المخترقة فيبقى منوطاً بسعة خيالهم فقط. هل يمكن تغيير قيمة عداد المسافة إلى صفر وعداد السرعة إلى 160 وسيارتك متوقفة؟ هذا سهل. وتشغيل زمور السيارة؟ أو تدمير جهاز الراديو؟ شد حزام الأمان؟ تشغيل مسّاحات الزجاج الأمامي؟ كلها أشياء بسيطة. وإيقاف تشغيل المحرك أو إدارة المقود إلى أقصى اليسار بحيث تفقد السيطرة على سيارتك عند القيادة بسرعة عالية؟ نعم، هذا ممكن. واستخدام أكياس الهواء في سيارتك فجأة لتفقد السيطرة وتنقلب مع أطفالك الجالسين في المقعد الخلفي؟ أمرٌ ممكنٌ جداً. عندما يتحكم حاسب بسيارتك، يمكن أيضاً للمهاجم أن يتحكم بها.

يكمن التحدي الذي تفرضه نقاط ضعف كهذه، في أن الهجمات لا تحتاج لاستهداف سيارة واحدة، بل يمكن أن تطال في الوقت نفسه كافة السيارات المتماثلة من حيث الصنع والنموذج وسنة التصنيع. ففي حالة مركز تكساس للسيارات، تمكن موظفٌ مارق من تعطيل مئات السيارات عن

بعد. لكن شركاتٍ مثل الشركة المنتجة لـ أُن.ستار تنصّب عمداً في ملايين السيارات تقنيات قادرة على إعاقة تشغيل المحرك عن بعد وشلّ حركة السيارة أثناء سيرها في حال تعرضت للسرقة. ألا يمكن إذاً لموظفٍ محتال في أُن.ستار أن يطفئ محركات مئات الآلاف، لا بل الملايين من السيارات؟ ومع أن جي.إم ستنكر ذلك بلا شك، فإنه ما إن يزرع هذا الباب الخلفي في السيارة، حتى تصبح حمايتها من الاستغلال تحدياً حقيقياً ويصبح من الممكن تعرضها لطيف واسع من هجمات البنى التحتية التي يمارسها المخترقون والدول القومية على حدٍّ سواء.

بينما تتكاثر شبكات أجهزة الاستشعار المحيطية وتتحسن تقانة العربات، سيوكل البشر المزيد من التحكم في مسؤوليات القيادة إلى الآلات. وقد صرّح كارلوس غصن، المدير التنفيذي لشركة "رينو نيسان"، رسمياً بأن شركته ستطرح سيارة ذاتية القيادة مستقلة بشكلٍ كامل في سوق المستهلك بحلول عام 2020، وتخطط شركة "فولفو" لتصنيع مثل هذه السيارات بحلول عام 2017. أما أكبر المناصرين لهذه التقانات فهي شركة غوغل، التي سجلت اختبارات سياراتها الذاتية القيادة أكثر من 700,000 ميل بدون أي حادث أو اصطدام. وهذه النقطة مهمة جداً لأن البشر، على ما يبدو، سائقون مروّعون ولأن أكثر من ثلاثة وثلاثين ألف أميركي يقتلون سنوياً نتيجة حوادث السير. فمن شأن شبكة سيارات ذاتية القيادة مؤتمتة بالكامل وتعمل بشكلٍ جيد، أن تجنبنا آلاف الوفيات التي لم تكن ضرورية وأن توفر المليارات من النفقات الاقتصادية المترتبة عليها. وبينما تنحدر تكلفة هذه التقانات، عليك أن تتوقع أن يتم استبدال سائقي البريد السريع وسيارات الأجرة ببدائل ذاتية القيادة رخيصة غير تابعة لنقابة.

لكن السيارات الحديثة، سواء قادها الناس أو الذكاء الصنعي أو البيانات الضخمة أو شبكات أجهزة الاستشعار، ستبقى مجرد أجهزة حاسب على

عجلات مزودة بأنظمة بيانات غير آمنة تتواصل عبر بروتوكولات نقل قابلة للاختراق بشكل كامل. على هذا النحو، قد تكون الأمور أقل ورديةً مما يفترضه مناصرو السيارات الذاتية القيادة. فعندما تنضم غالبية السيارات لإنترنت الأشياء، لن يمضي وقتٌ طويل حتى يتمكن مهاجمٌ محتال ما من السيطرة على إحدى السيارات وتحويلها إلى سلاح من عدة أطنان من المعدن والزجاج والوقود القابل للانفجار. وبالطريقة نفسها التي تستهدف فيها شركة الجريمة والعشاق السابقون المخبولون أجهزة الحاسب والهواتف النقالة، من المنطقي في المستقبل أن يتوجه هؤلاء نحو السيارات أيضاً ليجعلوا مشاهد مثل تلك التي ظهرت في فيلم التشويق المرعب للكاتب ستيفن كينغ عام 1983، الذي تدور أحداثه حول سيارة مسكونة اسمها "كريستين" أقرب إلى الواقع. ومن الواضح أن المسؤولين عن تطبيق القانون يدركون هذا التهديد، فقد حذر مكتب التحقيقات الفدرالي في تموز عام 20 في تقريرٍ داخلي من أن السيارات الذاتية القيادة قد تستخدم كـ "أسلحة فتاكة، حيث من الممكن أن يقوم الإرهابيون بملء السيارة الذاتية القيادة بالمتفجرات وتسييرها إلى وجهة معينة". ومن الممكن توقيف السيارات الذاتية القيادة بشكل جماعي لشل حركة المرور في مدينةٍ أو بلدٍ ما بشكلٍ تام.

لا شك في أن بعض الهجمات المركبية يتطلب درجة عالية من المعرفة بالحاسب، لكن كما رأينا في حوادث أخرى، ستتوافر قريباً برمجيات إجرامية تعمل بطريقة "أشر وانقر" لاختراق السيارات أيضاً. وقد بدأ صانعو السيارات بملاحظة الأمر، لا سيما بعد صدور قوائم "أكثر السيارات قابليةً للاختراق". فمثلما كان يتم تقييم السيارات بناءً على مدى قدرتها على تجنب الحوادث في الماضي، يصنّف الباحثون الأمنيون السيارات اليوم ليحددوا أكثرها قابلية للاختراق (والجواب هو "جيب شيروكي" و"كاديلاك

إسكالايد" و"إنفينيتي كيو50" و"تويوتا بروز"). واستجابة لهذه الهواجس المتنامية، قامت تيسلا، وهي الشركة المصنّعة لبعض أكثر السيارات تقدماً من الناحية التقانية على الطرقات اليوم، بتوظيف مستشارٍ أمني رفيع المستوى كان يعمل لدى شركة "آبل" لتحسّن موقعها. ولكن ما هي التهديدات الجديدة التي ستصبح قائمة عبر هذه التقانات المستقبلية عندما تسيطر شركة الجريمة عن بعد على سيارتك الذاتية القيادة وتقفل أبوابها وتسير بك مسرعةً إلى أحد المستودعات النائية على الجانب الخطأ من البلدة؟ ستحاول بالطبع الهروب من دون جدوى، لكن آخر ما سيسجله الشهود هو مشاهدتك تصرخ مرعوباً وأنت تضرب بقبضتك على الزجاج الداخلي للسيارة، عاجزاً عن مواجهة الجيل الثاني من عمليات الخطف. ولو افترضنا أنك نجوت بسيارتك الواقعة تحت سيطرة أحد المخترقين ووصلت حياً إلى البيت، فستكون مشاكل أخرى بانتظارك طبعاً، فبينما كنت في الخارج، انضم منزلك أيضاً لإنترنت الأشياء.

بيتي السعيد، بيتي المخترق

لقد كنّا على وعدٍ منذ أيام مسلسل "آل جيستون" بمنزلٍ من عصر الفضاء مليءٍ بالبدع الآلية والإلكترونيات الغريبة التي صنعت لكي تضمن حياة جيدة، وكل ذلك بكبسة زر. ومع أننا لم نحصل بعد على سياراتنا الطائرة، فإن المسلسل الكرتوني "هانا باربيرا" في بداية الستينيات مثّل نبوءةً عندما تنبأ بوجود التلفزيونات المسطحة ودردشة الفيديو والأبواب التي تنزلق آلياً. تبدو البيوت الحديثة المتصلة بالشبكة أمراً رائعاً من الناحية النظرية. فستحمينا الأنظمة الأمنية وكاميرات الفيديو من اللصوص وستتصل بالشرطة إذا تم كسر إحدى النوافذ. وستتفاعل موازين الحرارة الرقمية مع تقارير الطقس التي تصل لنظام الموقع الجغرافي العالمي وتنسق معه لتقوم بتعديل التدفئة والتكييف بذكاء لتضمن أعلى درجة من الفعالية والراحة

وادخار النفقات.

ستكشف أجهزة الاستشعار الذكية في القبو عن تسرب الماء إلى الأرض عند انفجار أحد الأنابيب، وستوقف جريان الماء إلى المنطقة المتضررة من الأنبوب تلقائياً. سيقوم هاتفك الذكي بقفل مزلاج الباب بوساطة الإنترنت، وبهذا لن تضطر للتساؤل أبداً وأنت في طريقك إلى المطار ما إذا كنت قد تذكرت القيام بذلك أم لا. ستقوم البرادات الذكية بتحذيرنا عندما يكون الحليب على وشك الفساد، كما أن فعلاً بسيطاً كرمي علبة "تشيريوس" الفارغة في القمامة، سيؤدي تلقائياً لاستخدام تفاصيل بطاقة ائتمانك لطلب المزيد من الحبوب بدون حتى أن ترفع إصبعك. ولكن هل تودّ حقاً أن يكون رقم بطاقة ائتمانك بحوزة سلة القمامة؟

"من المتوقع أن تصل قيمة سوق أتمتة المنزل في الولايات المتحدة إلى 16.4 مليار دولار بحلول عام 2019"، وكافة شركات التقانة الكبرى تتنافس على حصة لها. وقد تكون بعض عناصر منزلك قد انضمت بالفعل لإنترنت الأشياء، مع تزايد عدد مزودي الخدمات الذين يركّبون موازين ذكية لقياس وتنظيم استخدام الماء والكهرباء والغاز. ولكن ربما تكمن أكبر الفرص في مجال منتجات المستهلك، حيث تتصارع كل من جوجل وآبل وسامسونغ ومايكروسوفت، على سبيل المثال لا الحصر، لتكون المحور عبر تقديم نظام التشغيل المنزلي المركزي الذي يتيح لك إمكانية مراقبة مسكنك المتواضع والتحكم به باستخدام منفذ أتمتة المنزل أثناء تنقّلك.

لقد نجح منتج هوم.كيت من آبل الذي تم الكشف عنه مؤخراً في نقل أسلوب التصميم المميز للشركة العملاقة المتمركزة في مدينة كوبرتينو إلى مجال أتمتة المنازل، متيحاً للمستخدمين إمكانية قفل أبوابهم وتخفيف ضوء مصابيحهم وتشغيل مكبرات صوتهم بمجرد النقر على هواتف الآي.فون أو عبر إملاء طلبهم للمساعد الصوتي الذكي سيري. فبمجرد قولك

عبارة "ذاهب للنوم"، سيعلم نظام هوم.كيت أن عليه القيام بسلسلة من الأفعال، مثل إسدال الستائر وخفض درجة الحرارة وإطفاء النور، ولكن بالنظر للتجربة التي خاضها البعض مع تقنية التعرف الصوتي لدى سيري، لا يخلو الأمر من بعض المرح عندما يومض التلفاز فجأة أو تقلع السيارة ويُفتح بابها الأمامي. لكن مكامن الخلل سيتم إصلاحها على الرغم من كل شيء، كما أن إدارة المنافذ الرقمية المركزية في منازلنا بوساطة هواتفنا الذكية ستصبح حقيقة واقعة في المستقبل القريب جداً. فما الذي يمكن أن يحدث؟

لم يسبق لك على سبيل المثال أن اضطررت يوماً لتحديث البرنامج الثابت في غسالتك، أو لإعادة تحميل نظام تشغيل منزلك وإعادة إقلاعه لكي تتمكن من تشغيل الباب الرئيسي. فبينما قد يؤمن ربط المصابيح وآلات تحميص الخبز والغسالات ومسجلات الفيديو الرقمية والألعاب، والبرادات وأجهزة الاستقبال والأفران وغسالات الصحون والتلفزيونات وأقفال الأبواب وأنظمة الأمن وكاميرات مراقبة الأطفال، وموازين الحرارة والحمامات والمصابيح وأحواض الاستحمام بإنترنت الأشياء راحةً وملاءمةً كتلك التي لدى "آل جيتسون"، فإن ضمَّ كل هذه الأغراض لإنترنت الأشياء سيأتي مترافقاً مع تشكيلة خاصة من مخاطر الخصوصية والأمن. إذ لا تستخدم العديد من هذه الأجهزة أي تشفير ولا تجري عمليات تحقق من الهوية عندما تتواصل في ما بينها أو مع هاتفك النقال أو مع نظام المنزل. ونتيجة لذلك، سيكون من الممكن التلاعب بها واختراقها واعتراضها وتخريبها بسهولة. وقد وجدت دراسة قامت بها شركة إتش.بي في تموز عام 2014 أن 70% من الأجهزة المتصلة بإنترنت الأشياء غير منيعة أمام الهجمات، حيث يحتوي كل غرض على خمسة وعشرين عيباً مميزاً كحدٍّ وسطي.

حالما يصبح منزلك متصلاً بالإنترنت بشكلٍ كامل، لن يعود هناك سببٌ

للاعتقاد بأن المخترقين لن يعتبروه هدفاً مناسباً، وكل الدلائل تشير إلى أنهم يتحضرون بالفعل لاستهدافه. ولكل مهاجم أو مهاجمة دوافعه، ابن الجيران الذي قلت له أن يبتعد عن حديقة منزلك، أو حبيب سابق غيور، أو توم المتلصص الذي لمح امرأة مرة عند محل البقالة، أو الحكومات الأجنبية الساعية لاستغلال إمكانات التجسس الافتراضي. أما بالنسبة لشركة الجريمة، فغالباً ما تكون المسألة مسألة مال، وهي ستقوم باستغلال الضعف في أجهزة إنترنت الأشياء في منزلك للوصول أية بيانات قيّمة مخزّنة في شبكتك أو بغرض السرقة اليومية. أوه، ولا تنس كريبتو لوكر، برنامج الفدية الخبيث الذي يسيطر على الحواسب والهواتف المحمولة ويقفلها عبر تشفيرها. يمكنك أن تتوقع من الأوساط السرية الرقمية أن يبيع مجموعات من أدوات برمجيات الجريمة التي يمكنها أن تقفل عليك وأنت داخل أو خارج المنزل، وأن تجبرك على دفع فدية بعملة بيتكوين الرقمية إذا ما أردت استعادة منزلك والتمكن من تشغيله مجدداً.

قد يواجه أولادك التهديدات نفسها وهم يلعبون "بيت بيوت". إذ يقوم كبار صانعي الألعاب مثل ديزني وماتل منذ الآن بدراسة إنترنت الأشياء، وهناك عدد كبير من الدمى والحيوانات الدمية والروبوتات المصغرة المزودة بالوايفاي آتية إليك عبر "إنترنت الدمى". ولكن الدمى قابلة للاختراق أيضاً، أو على الأقل واحدة منها هي أرنب كاروتز التفاعلي البلاستيكي، والذي يمكن التحكم به عبر تطبيق للهاتف الذكي ويحتوي كاميرا وميكروفون ورقاقة معرّف راديوي. حيث تم اختراقه بما سمح للمخترق بمراقبة الطفل صاحب الدمية عبر الفيديو.

ثمة تقنيات أخرى، منها المصباح الكهربائي المعروف منذ 135 عاماً، تمر بتحّل إنترنت الأشياء. إذ تسمح نظم مثل نظام "فيليبس هيو ليد" للإنارة للمستخدمين بأن يطفئوا أو يشغّلوا الأنوار من هواتفهم الذكية. وتسمح

هذه النظم للمخترقين بأن يطفئوا أنوارك أيضاً، باستغلال عيبٍ أمني معروف ضمن نظام فيليبس، وهو أمر مقلق نظراً للعلاقة الواضحة بين النور والأمن الجسدي. وتقوم نظم أخرى، مثل مصباح التوفير الذكي إل.آي.إف.إكس، بتسريب كلمة السر لموجه شبكة الوايفاي في منزلك حالما يتم وصل المصباح بها، ما يكشفها أمام أي مخترق بمجرد توجيه استعلام إلى "المصباح الرئيسي" على شبكة منزلك. قد تحتوي المصابيح الكهربائية بدورها أبواباً خلفية كتلك الموجودة في المكاوي الصينية التي اكتشفت في روسيا. فقد صمم قراصنة في بداية عام 2014 مصباح تنصتٍ قادراً على إرسال محادثاتك الخاصة مباشرةً، ولا تتجاوز كلفة الجهاز الذي يعرف باسم كونفرسنيتش المئة دولار، وهو يشبه المصباح العادي؛ مع فرق وحيد هو أن هذا المصباح يحمل ميكروفوناً مخبأً يصغي لكافة الدردشات التي تحدث بالقرب منه. ولكي يثبتوا فعاليته، قام صانعو الجهاز بتسجيل فيديو يظهرون فيه وهم يضعون جهاز "كونفرسنيتش" في المكتبات والمكاتب ومطاعم ماكدونالد وأحد أفرع البنوك، بدون أي تدخل أو ملاحظة من قبل الموظفين، منذرين بظهور أداة جديدة للتجسس الصناعي باتت ممكنة بفضل إنترنت الأشياء.

بينما تتكاثر أجهزة إنترنت الأشياء الذكية، سيتم التحكم بها عن طريق البوابات المركزية لأتمتة المنازل التي بات من الممكن اختراق غالبيتها بما يسمح للمخترقين بالسيطرة على كافة الأجهزة في شبكتك المحلية. وسيصبح الأمر مثل فيلم الرعب "كابوس في شارع البيت المتصل بالشبكة". فعلى الرغم من أننا قد ننعم بنوم أفضل في الليل معتقدين أننا بأمان وسلامة في منازلنا المزودة بإنترنت الأشياء، فإن النسخة 2.0 من غزو المنزل سهلة التطبيق إلى حد مفاجئ، كما أثبتت كاشمير هيل مراسلة مجلة فوربس. فبينما كانت تعمل على قصة صحافية عن إنترنت الأشياء، كان كل ما قامت

به هيل هو البحث عن مصطلح "المنازل الذكية" على غوغل، فسرعان ما تمكنت من الكشف عن ثماني عائلات تستخدم نظام أتمتة المنزل الشائع إنستيون، الذي يتحكم بمعدات مثل "المصابيح وأحواض المياه الساخنة والمراوح والتلفزيونات وأبواب المرآب".

فقد تمكنت مراسلة فوربس من أيجاد منتجات أنستيون بدون صعوبة، لأن أنستيون لا يطلب اسم مستخدم أو كلمة سر، ولأنه جعل محركات البحث قادرة على إيجاد منتجاته. أجل، يمكن للناس الآن أن تجد برادك الذكي على غوغل وأن تتواصل معه من بعيد. تواصلت هيل مع الأطراف البريئة في المسألة لسؤالهم، فقدمت نفسها وقالت، "أستطيع أن أرى جميع الأجهزة في منزلكم وأعتقد أن بإمكاني التحكم بها". وطلبت إذنهم للقيام بذلك، فوافق أصحاب المنزل المرتعبون على مضض، بينما راحت المراسلة تتحكك بأجهزتهم بسهولة. ولم يكن مركز إنستيون وحيداً، فقد وجدت دراسة تم إجراؤها عام 2013 أن المخترقين استطاعوا بسهولة أن يقتحموا 80 بالمئة من مراكز المنازل الذكية الشائعة الاستخدام، ومن ضمنها فيرالايت كونترولر الذي يتوافق مع أكثر من 750 منتجاً للمنازل الذكية.

إن عدد نقاط الضعف الكامنة في نظم أتمتة المنازل كبيرٌ جداً إلى درجة أجبرت "فريق الجاهزية للطوارئ الحاسب في وزارة الداخلية" عام 2014 على نشر تحذيرٍ عام وجّه إلى 500,000 من مستخدمي جهاز المنزل الذكي الشائع ويمو من شركة "بيلكينز"، يحدد خمس نقاط ضعف منفصلة في المنتج. وورد في التحذير أن "مهاجماً مجهولاً قد يكون قادراً عن بعد على إدخال برامج ثابتة خبيثة أو نقل اتصالات خبيثة أو الوصول إلى ملفات نظام الجهاز، ليضمن الوصول التام للجهاز". وأضاف قسم الأمن الداخلي "ليس لدينا حتى الآن أي حل عملي لهذه المشكلة". وذكر تقرير عن الحادثة أنه "ما إن يقوم المهاجم بتأسيس اتصال مع جهاز ويمو ضمن شبكة

اتصال الضحية [،] حتى يصير بالإمكان استخدام الجهاز كموطئ قدم بغرض مهاجمة أجهزة أخرى مثل الحواسب المحمولة والهواتف النقالة وأجهزة تخزين الملفات المتصلة بالشبكة". إن التحذير الأخير مهمٌّ جداً. لن يحاول المخترقون اختراق أكثر الأجهزة أماناً في شبكتك، مثل الحاسب المحمول المغلق والمشفّر باستخدام برنامج جدار ناري. بل سيتوجهون بدلاً من ذلك إلى أضعف الروابط، كغلاية قهوة ويمو الموثوقة القادرة على الاتصال بالإنترنت عبر شبكتك المنزلية، التي تستخدم بروتوكولات أمنية غير كافية إن وجدت. وحالما يخترقون غلاية القهوة، فإنهم يكسرون خط دفاع ماجينو الافتراضي المحيط بشبكتك، وعندها يصبح كل ما يحتاجون إليه هو الوثب والتخطي والقفز لإصابة ومهاجمة الأجهزة الأخرى الأكثر أماناً وأكثر تحقيقاً للربح في منزلك.

يمثل نظام الإنذار الأمني أحد أكثر الأشياء المتصلة بالإنترنت شيوعاً في المنازل والشركات، ويعتمد أكثر من ستة وثلاثين مليون أميركي على هذه الأنظمة للحفاظ على أمن أنفسهم وأمن عائلاتهم. ولكن سواء كان الأمر متعلقاً بجهاز الاستشعار الخاص بالباب أو بلوحة المفاتيح، فكلاهما يمكن اختراقه بسهولة، مثلما شاهدنا في كل أفلام "المهمة المستحيلة" الهوليوودية. إذ تستخدم غالبية نظم الإنذار، ومن ضمنها أنظمة من شركات مثل أي.دي.تي وفيفينت، بروتوكولات اتصال لا سلكية قديمة تعود للتسعينيات، عاجزة عن تشفير أو مصادقة إشارات الإرسال الخاصة بها. لذا فقد تنقلب كاميرات هذه الأنظمة التي صممت بغرض الحماية على أصحابها بأن تتجسس على أنشطتهم وتعطّل أجهزة إنذارهم بحيث تعجز عن الإقلاع عندما يدخل غريبٌ إلى المنزل.

لا تقتصر نقاط الضعف على أنظمة الإنذار الأقدم، إذ يمكن أيضاً اختراق بروتوكولات إنترنت الأشياء الحديثة للاتصال الراديوي مثل أجهزة موجة زِد.

وهو أمرٌ مقلق نظراً لوجود 160 مصنّعاً يستخدم هذه البروتوكولات، وهي معتَمَدة في آلاف الشركات مثل لاس فيغاس وين هوتيل، الذي يستخدم خمسة وستين ألف جهاز يعمل بموجات زد في غرف نزلائه. وقد أعلنت سلسلة فنادق هيلتون أيضاً خططاً للسماح للزبائن باستخدام هواتفهم الذكية كمفاتيح لفتح غرفهم في أربعة آلاف فندقٍ عبر العالم بنهاية عام 20. ومع اتصال المزيد من أقفال أبواب المنازل ومزاليجها بالإنترنت، قد تفتح هذه المنازل أبوابها للإصدار الثاني من غزو المنازل، ليصبح المحتالون قادرين على اختراق وفتح باب منزلك عبر هواتفهم الذكية وتعطيل أجهزة الإنذار في بيتك ليتأكدوا من أن أحداً لن يسمعك صرخاتك في هذه المنازل.

لن تقتصر حوادث الاختراق على منافذ أتمتة المنازل المركزية وحسب، بل ستمتد إلى الأجهزة الذكية المنفردة مثل التلفزيونات. وتشير العديد من التقارير بالفعل إلى أنك حين تجلس لمشاهدة التلفزيون الذكي، قد يكون هو بدوره يقوم بمشاهدتك. إذ تُصمم غالبية أجهزة التلفاز اليوم، سواء كانت ذات نطاق متوسط أم عالي، بحيث تكون متوافقة مع إنترنت الأشياء، كما يتم تحميلها مسبقاً بتطبيقات مثل نيتفليكس وسكايب وفايسبوك وهولو، ناهيك بالكاميرات المدمجة والميكروفونات ومنافذ يو.إس.بي. وقد تم بيع نحو تسعين مليون تلفاز ذكي عبر العالم في عام 2013، وسيكون من الصعب قريباً إيجاد أجهزة التلفاز القديمة "الغبية"، وهو توجّه قد يكون مشكلة بالنسبة لأولئك الذين يقدرون الخصوصية والأمن. فقد تم كشف نقاط ضعف في العديد من الماركات، مثل أجهزة تلفاز سامسونغ الذكية التي سمحت للمخترقين بأن يقوموا بتشغيل الكاميرا المدمجة، المصممة من أجل مكالمات سكايب، عن بعد والتقاط الصور خلسةً ومشاهدة المتفرجين في غرف معيشتهم ونومهم.

كما تمكّن المخترقون من سرقة معلومات الدخول وتفاصيل الحسابات

المخزنة على تطبيقات أجهزة تلفاز سامسونغ الذكية، ليسيطروا على حسابات المستخدمين على فايسبوك وغيره من الوسائط الاجتماعية. وقد كانت هناك مفاجأة أخرى غير سارة لهؤلاء المستخدمين المطمئنين الذين استخدموا منافذ يو.إس.بي الخاصة بالتلفاز الذكي، لوصل قرصٍ صلبٍ خارجيٍ للتمكن من نقل الموسيقى والفيديو مباشرةً إلى التلفاز. فقد تمكّن المخترقون من رؤية وتحميل ومحو هذه الملفات عبر التلفاز، وهي أخبار سيئة لأولئك الذين يخزّنون أية ملفات ماليّة أو شخصية على أقراصهم الصلبة الخارجية. فهذه الاتصالات الإضافية داخل المنزل تجعل المستخدمين عرضة لهجوم من النوع الذي تعرض له الكاتب "مات هونان"، حيث يمكن محو الصور القيّمة وغيرها من البيانات المخزّنة محلياً عن بعد من قبل شخص سيّئ النية.

تجري كل من شركة الجريمة ووادي السيليكون على حدٍّ سواء تجارب تهدف للتوصل إلى أفضل الطرق لتحويل إنترنت الأشياء إلى نقود. وقد قام كل منهما في هذا السياق بتحديث تكتيكاته المجرّبة والموثوقة استعداداً لحقبة الحوسبة المحيطية. فقد كان القراصنة في بداية عام 2014 يسيطرون على أكثر من 100,000 غرضٍ "ذكي" من أغراض الحياة اليومية، من بينها موجّهات الشبكات المنزلية وأجهزة الإنذار ضد السرقة وكاميرات الويب ومشغّلات الملتيميديا والبرادات، فقاموا بتجميعها لتشكل أول شبكة روبوتية للأجهزة المنزلية المخترقة في التاريخ. واستخدم المهاجمون هذه الأجهزة ليرسلوا "أكثر من 750,000 رسالة بريد إلكتروني خبيثة وتصيدية" كان الهدف من كلٍّ منها هو تحقيق الربح لشركة الجريمة. ربما كان بريد الثلاجات المزعج (غير القابل للأكل) مشكلةً بحد ذاته، لكن من المهم أن نتذكر أن هذه الأجهزة هي عبارة عن أجهزة حاسب كاملة الأركان، قادرة على القيام بكل ما يقوم به الحاسب الثابت المُخترق حالما يتم اختراقها،

بدءاً من تخزين صور إباحية للأطفال وصولاً إلى إغراق مواقع إلكترونية مستهدفة بأحجام كبيرة من البيانات غير المفيدة. وإذا كان ربط مليون حاسب من حاسبات اليوم ضمن جيش من الروبوتات المخترقة أمراً سيئاً بما فيه الكفاية، فإن إضافة خمسين مليار جهازٍ ذكي إضافي إلى الشبكة تعاني كلها ضعفاً أو غياب الأمن، ستفتح فرصاً مذهلة للهجمات الحاسوبية العدوانية.

ستكبر الشبكات الروبوتية ويزداد حجمها من ملايين الآلات المُخترقة إلى البلايين منها، لتجلب معها صيغاً جديدة من أسلحة الدمار الشامل. وستستحوذ شركة الجريمة عبر استخدامها لهذه الأسلحة الافتراضية على أدوات فعالة جديدة في ترسانتها لابتزاز الشركات والأفراد على حدٍّ سواء، وإبقائهم دون اتصال بالشبكة إلى أن يتم دفع "الجزية" بالعملة الرقمية. ويمكن للطاقة الحاسوبية المدمجة في الأغراض الذكية المبعثرة في أرجاء منزلك ومكتبك أن تكون مربحة للمجرمين بطرقٍ أخرى أيضاً. فقد اكتشف الباحثون في بداية عام 2014 عشرات الآلاف من مسجلات الفيديو الرقمية التي تمَّ اختراقها بدودة "لينوكس.دارلوز"، بغرض استخدام قوة المعالجة لديها للتنقيب عن العملات الرقمية مثل "مين كوينز" و"ديغوكوينز". حيث يمكن للمخترقين بذلك أن يجعلوا أجهزتك تعمل بسرعتها القصوى، مولدةً عملاتٍ افتراضية لصالحهم بينما تتحمل أنت نفقات الكهرباء الناتجة عن تشغيل جهازك على مدار الساعة. يمكن نظرياً للعداد الذكي الجديد في منزلك أن يكتشف الاستهلاك الزائد في الطاقة، ولكنه بدوره قابل للاختراق بالطبع.

ما تعلمُهُ المنافذ

ستحتل العدادات الذكية مكاناً لها في قلب إنترنت الأشياء العالمي، وستسمح اتصالاتها الثنائية المسار بتسجيل وتعقب تفاصيل استهلاك

الكهرباء في المنازل والشركات بهدف زيادة كفاءة وموثوقية شبكة الكهرباء المثقلة التي عفا عليها الزمن. ففي بداية عام 2013، كان قد تم تركيب عدادات ذكية في أكثر من ستة وأربعين مليون منزل في الولايات المتحدة، ومن المتوقع اعتمادها في كافة أنحاء بريطانيا بحلول عام 2020. ويمكن للمعلومات القادمة من العدادات الذكية التي يتم نقل معظمها بصيغة غير مشفّرة، أن تكشف بالفعل نوع وعمر أجهزتك ومتى تستخدمها وفي أية غرفة في منزلك. وسيكشف استقراء مثل هذه البيانات كم من الوقت تستغرق في الطهو ومتى تقوم بتشغيل التلفاز في غرفة نومك. لكن عمق التفاصيل التي يمكن أن تؤمنها العدادات الذكية حول أنشطتك يمتد إلى ما هو أبعد من مجرد معرفة أنك استخدمت المايكرويف في الساعة 7:26 مساء يوم الخميس.

كشف باحثون في ألمانيا أن أجهزة التلفاز الذكية يمكن أن تخبرنا بالبرامج التلفزيونية التي يتابعها الناس وبتوقيت مشاهدتها، وفقاً لكمية الكهرباء المطلوبة لتشغيل المشاهد الخاصة بكل برنامج على شاشتك. وقد تمكّن الباحثون من إنشاء ملفات مخصصة لكل برنامج تلفزيوني بعد قياس كميات الكهرباء بالإجمال، ليتبيّن أن الحلقة 71 من ستار تريك تملك إشارة طاقة مختلفة عن تلك التي تملكها الحلقة 17 من "مودرن فاميلي". وثمة بالطبع مليارات الدولارات التي يمكن جنيها مقابل بيع هذه البيانات لأطرافٍ أخرى. وقد أعلنت شركة دبليو.بي.بي، وهي أكبر شركة إعلانات في العالم، في أيار عام 2014 بالفعل، تعاونها مع شركة أونزو لتحليل البيانات في لندن لدراسة الطرق الممكنة، لجمع بيانات العدادات الذكية بهدف "فتح باب المنزل" أخيراً للمعلنين.

يمتد التهديد الكامن وراء العدادات الذكية إلى ما هو أبعد من أثرها العميق على الخصوصية، إذ يهاجم المجرمون أجهزة الخدمات الذكية غير

الآمنة للعديد من الأسباب، وأهمها الاحتيال المالي. ففي بورتوريكو على سبيل المثال، وظّفت شركة الجريمة فرقاً كبيرة من عصابات التقانة لاستغلال الانتشار الواسع للعدادات الذكية في الجزيرة. وبدأ المخترقون المجرمون بإجراء "اتصالات خدمة" مع الشركات والأفراد على حدٍّ سواء، باستخدام برامج متوافرة بكثرة في الأوساط الرقمية السرية وحاسب محمول بسيط. فنجحت شركة الجريمة في برمجة العدادات الذكية بحيث توفر على "زبائنها" مقداراً يصل إلى 75% من فواتير الكهرباء الشهرية الخاصة بهم، مقابل رسومٍ تتراوح بين 300 إلى 1000 دولار لأصحاب المنازل من العملاء، و3000 دولار لأصحاب الشركات. ووفقاً لما ذكره تحقيقٌ عن الحادثة أجراه مكتب التحقيقات الفيدرالي، فقد خسرت سلطات الطاقة والكهرباء البورتوريكية التي تضررت من هذه الحادثة نحو 400 مليون دولار من عائداتها السنوية نتيجة لذلك. فالعدادات الذكية، كغيرها من الحواسب، غير منيعة أمام الهجمات الخبيثة. وقد ابتكر الباحثون في المجال الأمني في شركة آي.أو.أكتيف دودة قادرة على الانتشار بسرعة من عدّاد ذكي مصاب في أحد المنازل لآخر مما يمكنها من إصابة حيٍّ كامل وإغراقه في الظلمة.

يعمل مقياس الحرارة الذكي المعلّق على حائط منزلك يداً بيد مع عداد الخدمات الذكي، وثمة شركة واحدة تبزّ جميع الشركات الأخرى في إحداث الثورة في هذا المجال، هي شركة نيست لابس التي أسسها مديران تنفيذيان سابقان في شركة آبل. فقد أعاد منتجها نيست اختراع ميزان الحرارة القديم، والذي لم يتغيّر كثيراً منذ الخمسينيات، بشكلٍ كامل. حيث ابتكر مؤسسو الشركة ميزان حرارة جميلاً مزوداً باتصال وايفاي وأجهزة استشعار متطورة حساسة للحرارة والرطوبة والضوء وقادرة على كشف الحركة، مستفيدين في ذلك من خبراتهم الهائلة في مجال التصميم التي حصدوها أثناء عملهم في شركة آبل. ويستخدم نيست خوارزميات ذكاء صنعي تكيّفية تم تصميمها

بحيث تعلم ما هي درجات الحرارة التي تجعلك سعيداً ومتى. ويقدم نيست أيضاً نمط الخروج التلقائي الذي يكشف عدم وجود حركة أو ضوء بالقرب من الجهاز، ليستنتج بشكل صحيح أنك في عطلة أو أنك لست في المنزل. لقد أصبحت موازين "نيست" لقياس الحرارة منتشرة جداً بين الناس، كما أن مئات الآلاف من الوحدات تختفي من رفوف المحالّ شهرياً إلى جانب منتجات نيست الأخرى، مثل جهاز الاستشعار للإنذار ضد الحرائق المتكلّم المتعدد الاستخدامات والمزود بتقنية إنترنت الأشياء واتصال وايفاي. لم تمرّ الحماسة الواسعة أمام شركات التكنولوجيا الضخمة الأخرى مرور الكرام، ففي عام 2014، قامت غوغل بشراء نيست بعد بضع سنوات فقط من تأسيسها. إنها أخبار جيدة لمؤسسي "نيست" وموظفيها المئة أو أكثر، ولكن ما الذي قد يجعل شركة إعلانات على الإنترنت تشتري مصنعاً لأجهزة إنترنت الأشياء؟

ترى غوغل الفرص الكامنة وراء إنترنت الأشياء بوضوح، ويمثل "نيست" منتجاً مادياً قوياً يدعم طموحاتها في معركتها لتحقيق ما تسميه "البيت الواعي". فكاشفات الحرائق وموازين "نيست" لقياس الحرارة مع كل أجهزة الاستشعار المدمجة داخلها تعتبر مصدراً هائلاً للبيانات، ومثلما جلبت هواتف أندرويد النقالة فرصاً جديدة للإعلان وبيع البيانات، كذلك ستفعل منتجات "نيست" لابس. ولا يزال أمام غوغل الكثير من عمليات الشراء على أي حال، فقد أعلنت في حزيران 2014 أنها تقوم بشراء دروبكام، وهي شركة كبيرة ناشئة لكاميرات الفيديو الأمنية، بسعر 555 مليون دولار. وتقوم دروبكام بتصنيع كاميرات بلوتوث ووايفاي أمنية عالية الدقة تبث تسجيل فيديو مباشراً إلى تطبيقات الهواتف النقالة، كما ترسل تحذيرات بناءً على نشاطات يتم تحديدها مسبقاً حين تكتشفها هذه الأجهزة. ولن تملك غوغل بعد شرائها "دروبكام" معلومات بحثك على الإنترنت وبريدك

الإلكتروني وهاتفك النقال وخرائطك وموقعك وحسب، بل ستمتلك أيضاً معلومات عن تحركاتك داخل منزلك من خلال البث الحي لتسجيلات الفيديو. وهكذا سيترافق كل من ميزان الحرارة وجهاز الإنذار ضد الحرائق والنظام الأمني بقائمة طويلة من شروط الخدمة. فهل يمكن أن تكون الآثار على خصوصيتنا أكثر وضوحاً؟

يعتبر العداد الذكي غير الآمن سهل المنال بالطبع، فهو طريقة رائعة لمعرفة متى تغيب عن المنزل لفتراتٍ طويلة من الزمن. فبدلاً من البحث في منشوراتك على فايسبوك، سيستفيد لصوص الغد من تسجيلات الفيديو الخاصة بك وسيستجوبون برادك ليعرفوا متى كانت آخر مرة فُتح فيها بابه، أو سيسألون ميزان الحرارة ببساطة عما إذا كان يعمل حالياً في نمط العطلة الطويلة. لقد تم اختراق ميزان "نيست" للحرارة من غوغل بنجاح، بحيث يسمح بالفعل بكل ما سبق ليفسح المجال للمخترقين للوصول للجهاز عن بعد ومراقبة وجود المالك في منزله عبر كاشف الحركة المدمج، أو حتى تشغيل التدفئة باستطاعتها القصوى. وثمة منتج رئيسي آخر من "نيست" يعاني صعوبات وهو جهاز "نيست بروتيكت" للإنذار والحماية وكشف الدخان وغاز أول أوكسيد الكربون. وقد تم استرجاع 440,000 جهاز بسبب خلل برمجي يؤخّر تشغيل جهاز الإنذار في حالة وجود حريق فعلي. ولدى كاميرات "دروبكام" نقاط الضعف الأمنية الخاصة بها التي يمكن للمخترقين استغلالها لمشاهدة الفيديوهات عن بعد وتشغيل الميكروفون الخاص بالكاميرا، وإدخال تسجيل فيديو مزيّف إلى بث الفيديو الحي على الإنترنت في حال أراد اللصوص إخفاء أثرهم، كما في فيلم "أوشينز إيليفين". ومن نافل القول أن شركة الجريمة متعطشة لمعرفة كل ما تعلمه منافذ الكهرباء لديك: فقد تجد أنك مع كل مصباح وايفاي جديد أو قفل باب تشتريه، تقوم بتزويد المخترقين عن غير قصد بكل ما يحتاجون إليه

لإيجاد طرقٍ جديدة لاصطياد منزلك عن بعد.

الهجمات على الشركات واختراق المباني

تقفز الشركات بدورها إلى مركب إنترنت الأشياء لتوفير المزيد من النفقات. ومع أن غالبية الشركات تملك فعلاً مسؤولي أمن معلومات، فإنه من الصعب التنقل في أرض المعركة التقانية، أي المكتب. فمعظم الناس لا يعلمون أنه منذ عام 2002، أصبحت معظم الطابعات مزودة بأقراص صلبة داخلية تحفظ كل الملفات التي تتم طباعتها أو نسخها. ولأن العديد من هذه الأجهزة يتم بيعها أو تأجيرها في النهاية، فإن البيانات التي تحتويها عرضة للسرقة بشكلٍ كبير، كما أوضح تحقيق لقناة سي.بي.سي نيوز. فقد تكشّفت زيارة لأحد المستودعات في نيوجرسي عن ستة آلاف طابعة للبيع، مليئة بأسرار عميقة للحكومات والشركات. وقام الباحثون والمراسلون بشراء أربع طابعات فقط ليروا ما يمكنهم استعادته، وكانت النتائج فضائحية. فقد وجد المحققون "عشرات الآلاف من الملفات" من بينها "95 صفحة من شيكات الرواتب مع الأسماء والعناوين وأرقام الضمان الاجتماعي" و40,000 دولار على شكل شيكات مطبوعة و"300 صفحة تحوي على سجلات طبية لأفراد" من برامج "أفينيتي هيلث بلان"، تحوي كل شيء من وصفات الأدوية إلى تشخيصات السرطان، و"شكاوى العنف المنزلي المفصلة ولائحة بالمطلوبين من المعتدين جنسياً" تابعة لوحدة الجرائم الجنسية في قسم شرطة بوفالو، و"لائحة بأهداف غارة على أحد أوكار بيع المخدرات" من فريق مكافحة المخدرات هناك.

لا حاجة للقول إنه لم تعد هناك حاجة للوصول المادي للطابعات في عالم إنترنت الأشياء المتشابك، حيث بات ممكناً سحب الكثير من الملفات من الطابعات عن بعد. وقد تمكن القراصنة من الوصول إلى الطابعات المتصلة بالشبكة (والتي يكون أغلبها متصلاً بالإنترنت في جميع المكاتب الحديثة)

ومشاهدة ما تتمّ طباعته بالزمن الحقيقي. علاوة على ذلك، تم اختراق طابعات المكاتب، مثل إتش.بي ليزر جيت برو، عن بعد للوصول بطريقة غير قانونية إلى شبكة الوايفاي الخاصة بك والحصول على كلمة سر مدير الشبكة، والتي يقوم الجهاز بتخزينها كنص عادي غير مشفّر. وقد بين هجوم استهدف برنامج ثابت مدمج تم اكتشافه عام 2011 أن ملايين طابعات إتش.بي يمكن أن تستقبل عن بعد تعليمات تحديث من المخترقين، سمحت لهم بجعل هذه الأجهزة تعمل بجهدٍ عالٍ ما أدى لاشتعال النار فيها. حيث تمكن المخترقون من تسخين الطابعة بشكلٍ زائد، عبر استغلال ثغرة في عنصر الدمج في الآلة، ما أدى لاحتراق الورق الذي يمر عبر الجهاز واندلاع اللهب في نهاية الأمر. لقد أصبح من الممكن بفضل إنترنت الأشياء إحراق الأشياء على بعد آلاف الأميال. ولن أعتمد على كاشف الحرائق المتصل بإنترنت الأشياء لإنقاذي لو كنت مكانك، لأن أي قرصان يمتلك بما يكفي من الدوافع ليشعل مكتبك أو منزلك، سيقوم أيضاً بإطفاء أي نظام أمان لكشف الحرائق على الأرجح.

يمكن اختراق أدوات أخرى شائعة في المكاتب، منها أدوات عقد مؤتمرات الفيديو التي نجدها في معظم المكاتب وقاعات الاجتماعات، أي حيثُ تُناقش أكثر الأسرار خطورةً. فمثلما يمكن للكاميرات في منزلك أن تمنح المخترق نظرةً شاملة على نشاطاتك، كذلك تفعل تلك العيون الرقمية في مكان العمل. فقد أثبتت أنظمة مؤتمرات الفيديو، كالتي تنتجها كل من "بوليكوم" و"سيسكو"، والتي يشيع استخدامها في معظم المكاتب اليوم، بوضوح أنها غير منيعة أمام الهجمات. ولإثبات ذلك، كتب أحد المخترقين برمجية خطاطية لكشف أكبر عددٍ ممكنٍ من أنظمة مؤتمرات الفيديو غير الآمنة، وقد اكتشف خلال وقت قصير أكثر من "خمسة آلاف اجتماع في غرف اجتماعات تعود لشركات قانونية وشركات صناعة أدوية وتصفية نفط

ومراكز طبية". ومن بين تسجيلات الفيديو الحية التي استطاع الدخول إليها، كان هناك اجتماعٌ بين محامٍ وموكّله القابع في السجن، و"غرفة عمليات في مركز طبي جامعي، واجتماع لمناقشة الاستثمارات المالية حيث كانت تُعرض المعلومات المالية السريّة الخاصة بإحدى الشركات على شاشةٍ للعرض"، وحتى قاعة اجتماعات "غولدمان ساكس". أثبتت هذه التجربة أنه في المكتب أيضاً، عندما يكون كل شيء متصلاً، يكون الكل قابلاً للاختراق. يمكن للقراصنة الاتصال بالكاميرات والميكروفونات عن بعد وتشغيلها للتجسس عليك وعلى شركتك، فالعديد من أنظمة بوليكوم وغيرها من نظم مؤتمرات الفيديو تُباع وتُركّب وتتم صيانتها بدون تطبيق أية بروتوكولاتٍ أمنية جدية، كما أنها تكون معدّة مسبقاً بحيث تستجيب بشكل تلقائي لأي طلب.

في غضون ذلك، تنشغل فرق البناء حول العالم ببناء مبانٍ وناطحات سحابٍ ومستودعات ومصانع "ذكية" وتحديث تلك الموجودة سابقاً. فوصل أي بناء بالشبكة يمثّل فرصة توفير كبيرة للمالكين الذين يمكنهم أن يستثمروا بأنظمة الأتمتة المعقدة، ليوفروا نفقات الماء والكهرباء والغاز في مبانٍ تشعر بوجودنا وتعرف كيف تطفئ نفسها ذاتياً بما يتلاءم مع حركة الناس. ستتصل جميع أنظمة التدفئة والتهوية والتكييف الحديثة (إتش.في.أيي.سي) بالإنترنت، كما تتم مكاملتها مع مجموعة متنوعة من أجهزة الإنذار والاستشعار وقارئات البطاقات الأمنية والكاميرات وحتى الأجسام المادية، مثل آلات البيع وأنابيب المياه وبوابات مواقف السيارات والمصاعد، ليتم التحكم بها جميعها مركزياً من قبل أنظمة تشغيل إدارة المبنى. وثمة دلائل على هذه "التحسينات" في كل مكان، وفي العديد من مباني المكاتب الضخمة، مثل تلك الموجودة في مانهاتن، حيث لم تعد المصاعد تحتوي على أزرار رقمية مفردة لتختار الطابق الذي تريد الوصول

إليه. بدلاً من ذلك، أصبحت البيانات المشفّرة ضمن شارة المعرف الراديوي الرقمي الخاص بك، أو أجهزة التحكم الموجودة ضمن محطة مركزية أمنية هي من يحدد مسبقاً إلى أي الطوابق سيأخذك المصعد.

يمكن اختراق أنظمة إدارة المباني التجارية تماماً مثل منفذ الأتمتة في منزلك، وقد تكون النتائج مفاجئة عندما يحدث ذلك. فقد اخترق الطلاب في معهد ماساتشوستس للتقانة في نيسان من عام 2012 مبنى غرين بيلدينغ ذو الواحد والعشرين طابقاً، حيث مقرّ قسم علوم الأرض والغلاف الجوي والكواكب في الجامعة، واستخدموا نظامه الإلكتروني المخترق لخلق لعبة تترس عملاقة متعددة الألوان. حيث أتاحت لوحة مفاتيح لاسلكية للاعبين أن يحركوا الأحجار ويدوروها ويُسقِطوها بما يتناسب مع الأضواء في المكاتب متنوعة، وكانت نوافذ المبنى تبدو من الجهة المقابلة للشارع وعبر كامبريدج، تومض وتتحرك كما لو كان المخترقون يلعبون اللعبة الروسية الشهيرة. ولكن بينما يمكن لعمليات اختراق المباني أن تكون ممتعة، قد يكون بعضها الآخر مكلفاً جداً.

تتوحد اليوم الأنظمة التي كانت تعمل عبر التاريخ كوحداتٍ مستقلة، والاتصالات البينية البعيدة المدى لإنترنت الأشياء قد تثبت أنها من الصعب التنبؤ بها وتخطيطها وحمايتها. وتلجأ العديد من المنظمات اليوم للإدارة المركزية في ما يتعلق بنظم أبنيتها لمواجهة هذه التحديات، فهي تختار التعاقد مع متعهد أمني خارجي على سبيل المثال، ليشرف عن بعد على كل التسجيلات الأمنية لشركة معيّنة عبر العديد من المواقع. لكن عندما يتصل كل شيء بالشبكة، يصبح ممكناً إدارة خدمات أخرى بشكلٍ مركزي، ومن ضمنها أنظمة إتش.في.أي.سي، ومن بين الشركات التي تقوم بذلك محالّ "تارغت" للبيع بالتجزئة، التي أوكلت مسؤوليات التدفئة والتكييف لبائع يعرف باسم "فازيو للخدمات الميكانيكية" في بنسلفانيا. يتفاعل تقنيو

"فازيو" من مقرهم مع مزود "تارغت" ونظام الإدارة التعاقدي، وهو طريقٌ يؤدي إلى الشريان الأم تصعب على شركة الجريمة مقاومته.

عندما فتح أحد موظفي "فازيو للتقانة" من دون إدراك بريداً إلكترونياً تصيّدياً، يحوي مرفقاً فيه برمجية خبيثة (وكانت أحد الأشكال المصرفية لحصان زيوس الطروادي الذي تنتجه شركة الجريمة)، تسبب لنفسه ولباقي أفراد شركته بالإصابة. ولكن بفضل اتصال فازيو بشبكة الاتصال التابعة لمحالّ تارغت، أتاح الحصان الطروادي للمخترقين إمكانية التلصص على فريستهم النهائية: متاجر بيع التجزئة الضخمة لشركة تارغت. وكانت النتيجة هي الهجوم الذي ذُكر في الفصل الأول على تارغت والثغرة الهائلة التي أدت لتسرّب تفاصيل بطاقات الدفع والمعلومات الشخصية لـ 110 ملايين مستهلك أميركي. في اللحظة نفسها التي تمكّن فيها المخترقون من اختراق "فازيو للتقانة" وسرقة معلومات الدخول من أحد الموظفين هناك، أصبحوا قادرين على استخدامها للبحث والاصطياد في شبكة تارغت إلى أن يصلوا إلى غايتهم.

وهناك وجدوا معلومات عن منافذ مزودي تارغت وبيانات عن إدارة مرافق السلسلة. وفي نهاية المطاف، أدرك المخترقون أن هذه الأنظمة، وهو أمر مثير للصدمة، ليست منفصلة عن أنظمة تكنولوجيا المعلومات الكبرى الأخرى المستخدمة من قبل محل البيع بالتجزئة، ومن بينها أنظمة الدفع والأنظمة المالية. وبعد أن تزودوا بكل المعلومات التي يحتاجون إليها، انتشر المخترقون كالجرذان عبر العديد من الشبكات المترابطة، إلى أن وصلوا إلى مخدّم الشركة الداخلي المسؤول عن التحكم بعشرات آلاف محطات نقاط البيع الفردية، حيث يمرّر المستهلكون بطاقاتهم الائتمانية أمام العداد. وحالما وصل المخترقون إلى هذه النقاط قاموا بتحميل برنامج خبيث يعرف باسم "تروجان بوسرام" يقوم بنسخ كل البطاقات التي تمسح في

مخازن "تارغت" في كافة أنحاء البلاد وينقل البيانات بسرية إلى روسيا. واستمرت عملية الاحتيال الهائلة هذه إلى أن استطاع الباحث الأمني "براين كريبس" كشف القصة. لا شك في أن الهجوم على محالّ تارغت يعد أقوى هجوم يستهدف نظام إتش.في.أي.سي إلى يومنا هذا، لكنه ليس الوحيد.

قد نرغب بأن نصدق أنه كان يمكن للحكومة أن تقوم بعملٍ أفضل لحماية أبنيتها من الهجمات التي تتم عن بعد، لكن لا يبدو أنه ثمة دليل على ذلك، حتى في ما يتعلق بالمرافق التي كانت تعتبر من أشد الأبنية أماناً. فقد تمكن الباحثون عام 2011 من اختراق شبكة اتصال نظام التحكم الصناعي في المكتب الفدرالي للسجون والسيطرة على المباني عن بعد. وكان بإمكان المخترقين أن يفكوا قفل أبواب زنازين معينة أو حتى جناحٍ كامل لو أرادوا، بينما تصر شاشات أجهزة الحاسب في محطة الحراسة المركزية على أنها هذه الزنانين لا تزال موصدة. وكان من الممكن أيضاً إطفاء شبكة الاتصالات في السجن بحيث لا يتمكن للحراس من الاتصال للحصول على المساعدة في حالة الطوارئ. والأسوأ من ذلك أنه كان من الممكن "تدمير الأبواب" إلكترونياً، عبر تحميل نظام التحكم الإلكتروني الخاص بها فوق طاقته، وبالتالي ترك الأبواب مفتوحة بشكلٍ دائم لكل المساجين. فباستخدام هذه التقنيات، تستطيع شركة الجريمة تحرير شركائها لتعريض سجناء آخرين للخطر عبر فتح أبواب زنازينهم وتركهم عرضة لهجومٍ انتقامي. هذه المخاطر ليست نظرية فقط، ففي منتصف عام 2013 تسبب "خلل" حاسوبي غير معروف في مركز إصلاحية "تورنر غيلفورد نايت" في ميامي في مقاطعة فلوريدا، بفتح كل أبواب جناح الحراسة المشددة بوقتٍ واحد ليُطلق سراح السجناء، ما أدى لحدوث أعمال شغب وأتاح لأعضاء العصابات أن ينتقموا من خصومهم. ووفقاً لتسجيلات كاميرات المراقبة في

السجن، كان هناك سجينٌ واحدٌ بدا متحضراً للحادثة التي أذهلت الحراس والسجناء على حدٍّ سواء. ففي اللحظة التي فُتحت فيها الأبواب، مشى السجين بهدوء عبر الممر إلى زنزانة عدوٍّ قديم، وضربه بسكين يدوية الصنع قبل أن يعود لحجرته. وكان سبب "الخلل" لا يزال قيد التحقيق في أواخر عام 2014، لكن ما يمكن فهمه من هذه الحادثة هو أنه ليس على كل بناءٍ في مجتمعنا أن يكون متصلاً بالإنترنت.

تخلق مساحة التهديد المتزايدة الناتجة عن إنترنت الأشياء فرصاً لا تقتصر على شركة الجريمة وحسب، ولكنها تصل للحكومات القومية أيضاً، كما اكتشفت غرفة التجارة الأميركية. فبصفتها المجموعة التجارية التي تتصدر عمليات تضغط لمصلحة الشركات الأميركية، لطالما كانت الغرفة تتخذ مواقف تجاه العلاقات الدولية وقضايا التجارة الأجنبية، خصوصاً في ما يتعلق بالصين، بالنيابة عن أعضائها الذين يبلغ عددهم ثلاثة ملايين. وبينما تمكنت الغرفة من صد الهجمات الافتراضية التي استهدفت شبكتها الرئيسة والتي انطلقت من جمهورية الصين الشعبية في الماضي، لم يكن حظ الغرفة جيداً أواخر عام 2011، عندما اكتشفت وجود ميزان حرارة مزود بالإنترنت تم تركيبه حديثاً في أحد مكاتبها في "كابيتول هيل". فقد خلق هذا الميزان بدون قصد باباً خلفياً لشبكة الاتصال الداخلية في الشركة. وقد اكتشف مسؤولو الغرفة الأمر عندما وجدوا أن الجهاز الموفر للطاقة يقوم بالاتصال سريًّا مع عنوان على الإنترنت في الصين.

ربما كان المخترقون أذكياء عندما اختاروا ميزان الحرارة ليكون وسيلة دخولهم إلى شبكة الاتصال الرئيسة للغرفة، إلا أنهم لم يوفّقوا في توجيه مهام الطباعة. فقد تسبب إهمالهم في تشغيل طابعة يستخدمها مديرو الغرفة لتبدأ تلقائياً بطباعة صفحاتٍ تحتوي معلومات مكتوبة بأحرف صينية، الأمر الذي اعتبره المسؤولون في مكتب التحقيقات الفيدرالي دليلاً

كافياً على وجود عطل ما. لكن القراصنة، حالما صاروا داخل شبكة اتصال الغرفة، بدأوا بالبحث عن معلومات مالية أو تتعلق بالميزانية وعن أنظمة بريد إلكتروني مخترقة، وركزوا على الموظفين الذين يعملون في قضايا السياسات التجارية في آسيا. فنحن لا نخطئ إذ نقول بأن هناك آثاراً جيوسياسية عميقة لإنترنت الأشياء، والدول القادرة على استثمار هذه التقنيات لحدها الأقصى ستحصل على معلومات استخبارية وميزاتٍ استراتيجية غير مسبوقة. وكما أشار رئيس مجلس الدولة الصيني، "وين جياباو"، في خطابٍ له في آب عام 2009 في مدينة ووكسي: "الإنترنت + إنترنت الأشياء = حكمة الأرض".

نظام تشغيل المدينة الذكية

من لديهم خبرات الحرب يمكنهم قهر العدو بدون معركة.
يسيطرون على مدنه بدون الاعتداء عليها ويسقطون الدولة بدون عملياتٍ طويلة الأمد.
سن تسو

تنبأ المارشال مك.لوهان عام 1964 ببصيرته النافذة بأنه "بفضل الوسائط الإلكترونية... كل التقنيات السابقة... بما فيها المدن... [سوف] تترجم إلى نظم معلومات". ربما استغرق حدوث ذلك خمسين سنة، لكن نبوءته كانت دقيقة. فلدى إنترنت الأشياء القدرة التامة على تحويل المدن إلى نظم بيئية حية تتنفّس، مكوّنة من الذكاء المحيطي وأجهزة الاستشعار المترابطة، تضمن تحسين حياة ساكنيها تحسيناً كبيراً. وحسب الرؤية الطوباوية للمدن الذكية، ستُعلِم حاويات القمامة المزودة بأجهزة استشعار داخلها جامعي القمامة بامتلائها، ليتم إيفاد أقرب شاحنة قمامة مزودة بنظام الموقع الجغرافي لإزالة القمامة. وتستطيع شبكات أجهزة الاستشعار التابعة

للبلدية قياس مدى التلوث الذي ينتجه كل بناء ونوعية الهواء في حيٍّ معيّن أو عدد المشاة في شارعٍ معين، وبذلك يصبح لدينا أول جهاز "فيتبت لأجل المدينة" في التاريخ. وسيعني وجود حساسات أفضل في مصابيح شوارعنا، أن البلديات ستكون قادرة على تأمين الدرجة الصحيحة من الإنارة، والتي سيتم تعديلها بما يتناسب مع أوقات النهار والفصول وأحوال الطقس، ما سيخفض تكلفة الطاقة بما يعادل 30 بالمئة. كل هذا سيحدث بالطبع إذا سار كل شيء على ما يرام.

فإحدى وجهات النظر الأقل تفاؤلاً في ما يتعلق بنظام تشغيل يشرف على كامل المدينة، هي أن شبكات البلدية من الأجهزة المزودة بإنترنت الأشياء المتصلة دائماً بالإنترنت، ستكون عرضةً بشكل دائم للهجوم من قبل المخترقين من كافة أنحاء العالم. فباستخدام نظام كشف السيارات اللاسلكي الشائع الاستخدام في العديد من المدن حول العالم، تمكن القرصان الأرجنتيني سيزار كيرودو من التحكم بإشارات المرور في مانهاتن عبر اختراق الحساسات المدمجة بالشوارع، وهي تقنية سمحت له بإعادة توجيه حركة المرور والتسبب بالازدحام كما يريد. وقد يتسبب اختراق المباني ونظم تشغيل المدن بأضرار مادية أيضاً، كما أنه يسمح للمخترقين بالسيطرة على المصاعد وفتحات التهوية وأقفال الأبواب والإنارة والجسور والأنفاق ومرافق معالجة المياه وغيرها من الأنظمة الحيوية. إذا كان اختراق العدادات الذكية ممكناً، فهو أيضاً ممكن مع الشبكات الذكية. كما أن إمكانية قيام مجموعة من الناشطين - القراصنة أو عصابات جريمة منظمة أو فئة من المتمردين بفصل الطاقة عن عامة الناس أصبحت حقيقةً واقعة. فقد تمكّن باحثٌ في المجال الأمني في تموز عام 2014 من السيطرة على تمديدات الطاقة في إتلنغن، وهي مدينة في جنوب ألمانيا عدد سكانها يبلغ أربعين ألفاً. ويمكن لأي مخترق أن يقوم بالفعل نفسه ليوقف تشغيل

مرافق البلدية بما فيها الكهرباء والماء والغاز.

يحمل اختراع إنترنت الأشياء إمكانيةَ تحقيق تحسينات كبيرة على نوعية حياتنا وعلى الاقتصاد العالمي على حدّ سواء، وبخاصة عندما تصبح الأشياء "ذكية" وتتعلم كيف تتفاعل تلقائياً معاً لصالحنا. لكن وبغض النظر عن المخاوف الكبرى المتعلقة بالخصوصية الآن، فإننا نزوّد المخترقين بعددٍ لا محدود من نقاط الاتصال التي يمكنهم أن يقتحموا عبرها حياتنا لجعلها أسوأ عندما نمكّن بلايين السيارات وآلات صنع القهوة والمباني والهواتف المحمولة والمصاعد وغسالات الصحون والألعاب من التواصل معاً وتلقي الأوامر من الإنترنت بشكلٍ عام.

نحن عاجزون عن حماية الأشياء القليلة نسبياً المتصلة بالإنترنت اليوم، لكننا مع مرور كل يوم ندخل أشياء ذكية جديدة إلى منازلنا وحياتنا دون أن نكلف أنفسنا عناء التوقف والتساؤل عن المخاطر والمشاكل الكامنة فيها. نتيجة لذلك، يمكن للمخترقين أن يستغلوا وزن وقوة اتصالاتنا المتزايدة لهزيمتنا، مثلما يفعل ممارسو فن القتال القديم الجودو. لقد وصلنا العالم ببعضه، لكننا فشلنا في الحقيقة بجعله آمناً، وهذا قرار قد نندم عليه جميعاً، وخاصةً أننا قد بدأنا بوصل الجسد الإنساني نفسه بالإنترنت.

الفصل الرابع عشر
اختراقُكْ أنت

سيغيّر إنترنت الأشياء، أو ما يشار إليه أحياناً بإنترنت الأغراض، كل شيء، وبما في ذلك نحن أنفسنا.

ديف إيفانس، كبير رؤيوي في سيسكو السابق

"يصارع رائد الفضاء ستيف أوستن الموت. ولكن أيها السادة، يمكننا إعادة بنائه من جديد، فلدينا التقانة اللازمة. لدينا الإمكانية لصنع أول رجلٍ بأعضاءٍ آلية في العالم. سيكون ستيف أوستن هو ذلك الرجل. وسيكون بحالةٍ أفضل مما كان عليها سابقاً. أفضل وأقوى وأسرع". كانت تلك هي السطور التي كانت تُتلى في شارة بداية البرنامج التلفزيوني الناجح في السبعينيات "رجل الستة ملايين دولار". وكالكثير من الفتيان الذين كبروا في تلك الفترة، كنت مبهوراً بالقوة الخارقة والهائلة التي امتلكها البطل الخارق ذو الأعضاء الآلية، وكنت أتوق للركض بتلك السرعة، والقفز لذاك العلو، والرؤية لتلك المسافة. وبقدر ما كان الرجل ذو الأعضاء الآلية رائعاً، أكّد لي البالغون أن كل هذا مختلق، وأنه محض خيال جاءت به أكثر قصص الخيال العلمي جموحاً. ولكن، كما تعلّمت لاحقاً، يمكن للخيال العلمي أن يصبح حقيقةً علمية بسرعة.

قابلت بيرتولت مايَر لأول مرة في منتصف عام 2012، عندما كان يقوم بتصوير فيلمٍ تلفزيوني وثائقي للقناة الرابعة في المملكة المتحدة بعنوان "كيف تبني رجلاً بأعضاء آلية". وكان ماير، العالم النفسي الاجتماعي من جامعة زوريخ، والبالغ من العمر ثلاثةً وثلاثين عاماً، يستكشف الإمكانات والعواقب الأخلاقية لآخر تقنيات الأعضاء الآلية. ولم تكن اهتماماته هذه نابعة من الفضول العلمي وحده، بل من قدره الشخصي أيضاً، فقد وُلد ماير فاقداً للجزء الأسفل من ذراعه اليسرى. وخلال طفولته، تم تزويده

بأطراف صناعية بدائية مختلفة الأشكال، كانت كلها تجعله يشعر بأنه مختلف وتزعزع ثقته بنفسه، ناهيك بالإمكانيات الوظيفية المحدودة للغاية لهذه الأطراف. وكان طموح ماير هو امتلاك الفعالية التشريحية نفسها التي يمتلكها الآخرون، فكان يصبو إلى تجاوز يده التي لا تفتح والخطافات المعدنية التي تم تزويده بها عندما كان طفلاً إلى ما هو أبعد من ذلك. وتحقق الحلم عام 2009 عندما تم تزويده بأحد أكثر الأجهزة التعويضية تقدماً في الوجود: إنها يد "توتش بيونيكس آي - ليمب".

أصبح ماير رجل الأطراف الآلية في العالم الحقيقي. فقد كان مذهولاً من قدراته الجسدية الجديدة، كقدرته على التصفيق بيديه لأول مرة والإمساك بشوكة، وحمل حقيبة تسوّق ثقيلة بيده اليسرى. وكانت اليد الآلية الجديدة تشتمل على هيكل متطور من الألمنيوم بغرض "تحسين الديمومة وزيادة قوة القبضة والحصول على تصميم تشريحي صحيح" أكثر من أي طرف صناعي سابق حصل عليه. ويتحكم ماير بالجهاز عبر إرسال نبضات كهربائية عضلية من اللحم البشري الموجود فوق الطرف الصنعي تماماً إلى حساسات كهربية متصلة بجلده، تمكّن اليد من الفتح والإغلاق والدوران والتقاط الأشياء. كان هذا تطوراً هائلاً بالفعل بالنسبة لماير شخصياً أدى لاهتمامٍ عميق بعالم الأعضاء البديلة، موضوع فيلمه الوثائقي، حيث تم إجراء مقابلةٍ معي.

بينما كنت أتناقش مع رجل الأعضاء الآلية ومخرج الأفلام حول العواقب الأخلاقية لهذه التقنيات، تحولت المحادثة إلى موضوع الأمن الرقمي، وهو موضوعٌ لم يكن ماير قد أخذه في الاعتبار بعد. فكما تبين لاحقاً، لم تكن النبضات الكهربائية العضلية المرسلة من جسد ماير هي الطريقة الوحيدة لتشغيل اليد الآلية. فقد تم تزويد يده الآلية بتقنية البلوتوث، كما أنه يمكن التحكم بها وتعديلها وإعادة برمجتها بوساطة تطبيق على الهاتف

النقال قام ماير بتحميله من المصنّع على جهاز الآيفون الخاص به. ناقشتُ مع ماير نقاط الضعف الأمنية الكامنة والمعروفة في بروتوكول البلوتوث وكم من المرات تم فيها اختراقه من قبل القراصنة في الماضي. أدرك ماير فجأة عواقب نقاط الضعف الموجودة لديه، وتحول لونه إلى رماديٍ شاحب وتدلّى فكه دهشةً من نقاط الضعف التي لم يكشفها له أحدٌ من قبل.

طلبت من ماير أن أرى هاتفه المحمول والتطبيق الذي استخدمه للتحكم بيده الآلية. فاستجاب بأدب، وأعطاني الجهاز. وبينما كنت أتفحص تطبيق البلوتوث، وجدت أنه يؤمن العديد من الوضعيات للقبضة والخيارات البرمجية. فإذا نقرت على زر فستفتح يده، بينما يقوم زر آخر بإغلاقها. كما يمكن التحكم بوضعية كل أصبع بمفرده والمناورة بالإبهام والمعصم. كنت عندها أنا من يتحكم برجل الأعضاء الآلية وبكامل جسده. فبمجرد حيازتي هاتفه الذكي، صار جسد ماير الآن ينفذ أوامري. لم أكن بحاجة بالتأكيد لوصولٍ مادي لهاتفه، لأنه كان يستخدم بروتوكول البلوتوث غير الآمن. فكان يمكنني ببساطة اختراقه والسيطرة عليه عن بعد. وعلى الرغم من أن ماير لم يلاحظ ذلك، فقد انضمت يده إلى عالم إنترنت الأشياء، وبمجرد قيامها بذلك فإن استخدامها لم يعد محصوراً بمالكها الفعلي. بعد أن تجاوز ماير الصدمة الأولية، تابعنا نقاشنا وأصبحنا أصدقاء. كما أننا تعلمنا درساً هاماً معاً. فالآن، ولأول مرة في التاريخ، أصبح الجسد الإنساني بالذات عرضة للهجمات الافتراضية.

"كلنا سايبورغ الآن"

أنت تعلم، كل من يرتدي نظارات هو، بمعنىً أو بآخر، سايبورغ.

إيفينجي موروزوف

يستحضر مصطلح سايبورغ، وهو اختصار لـ "الكائنات السِبرانية"، صوراً لعالمٍ مرعب مسكون بأشباه البشر العدائيين، مثل كائنات سايلون في

"معركة الفضاء غالاكتيكا" وبورغ في "ستار تريك" أو السايبريون في "دكتور هو". وعلى الرغم من حداثة المصطلح، فإن محاولة التغلب على محدوديات الجسد الإنساني تعود لآلاف خلت من السنين، حين كان القدماء يستخدمون الخشب والنحاس والحديد لاستبدال أطرافهم المفقودة أو المشوهة. ومنذ ذلك الحين، قطعت التعويضات الصناعية شوطاً طويلاً، ليس فقط في تعويض الخسارة الوظيفية الجسدية الجزئية الناتجة عن الإصابة أو المرض، بل في تحسين إمكانات نظائرها البيولوجية التي تعمل جيداً. وقد برزت هذه التحسينات إلى الضوء مع العدّاء أوسكار بيستوريوس من جنوب أفريقيا، الذي حاز الميدالية الذهبية وهو مبتور الرجلين من أسفل الركبتين، فكان محط استهداف الكثير من الرياضيين الذين اشتكوا من أطرافه الصناعية الأشبه بأطراف كائنات فيلم بليد رنر التي أعطته ميزات غير عادلة.

لا تقوم التقانة اليوم بزيادة قدرات أطرافنا وحواسنا فقط، بل إن ذلك يشمل أدمغتنا أيضاً. إذ يذكر 90% من أصحاب الهواتف الذكية أن هواتفهم المحمولة تبقى على بعد 3 أقدام منهم على الأكثر في كل ساعات النهار، والنسبة مرشّحة للزيادة بالتأكيد في المستقبل. لا تعتبر هذه الأجهزة عقولاً خارجيةً فقط، بل أطرافاً وهمية أيضاً نتصل بها بشكل مستمر، ونقلق بشكلٍ كبير عندما تكون بعيدة أو عندما ننساها بدون قصد. فنحن نستخدم هواتفنا المحمولة كمصدر خارجي للذاكرة (يمكنها تذكّر آلاف الأرقام الهاتفية التي لا يمكننا نحن تذكرها) وكوسائل إضافية للتواصل، حيث نتشارك أفكارنا عبر الكوكب من خلال الرسائل النصية القصيرة وتغيير الحالة والتغريدات ورسائل البريد الإلكتروني. سنرتدي الأجهزة الذكية بشكلٍ متزايد، وسنقوم بتضمينها داخل أجسادنا في النهاية، وعندما يحصل ذلك، سننضم نحن أيضاً لعالم إنترنت الأشياء. ستتفاعل هذه الحواسب القابلة

للارتداء والأجهزة الطبية المزروعة والأطراف الآلية والهياكل الخارجية مع العالم من حولنا لتؤمن لنا قدراتٍ جسدية وذهنية جديدة، إلى جانب المراقبة المستمرة للصحة وأدوات المعلومات الراجعة. ومثلما ازداد عدد الرقاقات الصغرية في سياراتنا وتوحّدت في شبكة تحكم واحدة، سيحدث المثيل مع الأجهزة التي نرتديها والتي نحملها بداخلنا، فهي ستشكل شبكة الجسم الخاصة بها في المستقبل. وستأتي قضايا الأمن والخصوصية مع هذه التغيرات لتؤثر على إنترنت الأشياء الأوسع بشكلٍ كبير، ولكن في هذه المرة سنكون نحن مجرد عُقَد اتصال في شبكة الإنترنت.

سواء كان مستقبل "السايبورغ" مشابهاً بدرجةٍ كبيرة للرعب الذي تصوره رواية "فرانكشتاين" لماري شيلي، أو للقدرات البطولية التي نراها في الرجل الحديدي عند طوني ستارك ثمة أمرٍ واحد بات واضحاً على أي حال، فقد أظهرت شركة الجريمة مرةً بعد مرة قدرتها وعزمها على استثمار أية تقانة جديدة لمصلحتها، وقد يكون اختراقك واختراق جسدك فرصة جيدة لا تعوض.

أكثر مما يظهر للعيان: عالم الحوسبة القابلة للارتداء

ربما كانت سماعات الأذن هي أول أجهزة الحوسبة القابلة للارتداء التي حازت قبولاً كبيراً، وقد تحولت من وحدة ترانزيستور بسماكة رزمة أوراق اللعب يتم ارتداؤها على الصدر، وتبقى مرئية مع شرائط تحملها على الكتف إلى وحدة متكاملة مزودة بمعالج صغري، صغيرة بما يكفي لوضعها داخل قناة الأذن. من غير المفاجئ أن سماعات الأذن الحديثة تستخدم تقنية البلوتوث وقادرة على بث مصادر صوتية متعددة وتضخيمها من أجل فاقدي السمع. ويمكن للمستخدمين عبر تطبيقات الهواتف المحمولة أن يعدلوا ويتحكموا بالإعدادات على هواتفهم، ليختاروا أن يستمعوا إلى صوتٍ محيطي أو مكالمةٍ هاتفية أو موسيقى على الآيبود، كل هذا بكبسة

زر. لكن حتى سماعات الأذن المتواضعة اليوم، مثلها في ذلك مثل سماعات البلوتوث التي يرتديها عامة الناس، يمكن اختراقها باستخدام مجموعة متنوعة من برامج البلوتوث المتوفّرة في العالم السفلي التي سبق ذكرها. نتيجة لذلك، ليس من السهل اعتراض ما يسمعه شخصٌ آخر بشكلٍ فوري وحسب، بل من الممكن أيضاً إصدار أصوات أو ضجيج مباشرة في أذني الشخص الضعيف السمع. وسواء كان ما يبث هو موسيقى الميتال الثقيلة أو رسائل تهديد لا يسمعها سوى الشخص الذي يرتدي السماعات، من المؤكد أن هذه الأصوات ستسبب إزعاجاً وذعراً للضحايا.

انضمت إلى سماعات الأذن اليوم لائحة من الخيارات الإضافية، إذا ما نظرنا إلى أجهزة الاستشعار والتعقب والحواسب التي نرتديها على أجسادنا اليوم. وقد حدث العديد من هذه التطورات بفضل حركة "القياس الكمي للذات"، التي تستخدم العديد من المنهجيات لجمع المعلومات عن حياة الأفراد باستخدام الأدوات التقنية. ويقوم الملايين من أتباع حركة القياس الكمي للذات كل يوم بتسجيل كل أوجه حياتهم وأفكارهم وتجاربهم، بوساطة أدوات التعقب الذاتي بغرض الوصول لحياةٍ أفضل عبر "تسجيل الحياة". ويقوم هؤلاء بتعقب وقياس كمية نومهم ووزنهم والسعرات الحرارية التي يحرقونها وردود الفعل البيولوجية لديهم، ومعدل ضربات القلب والموجات الدماغية وإيقاع تخطيط كهربية القلب والسعادة وعدد الخطوات في اليوم، كل هذا ضمن الجهود الرامية لتحسين الأداء الذهني والجسدي، وقد بات من الممكن جمع هذه المعلومات بسهولة مع دخول أجهزة الحوسبة القابلة للارتداء والتي تعرف باسم "ويرابلز".

تسمح هذه الأجهزة لمن يتّبعون حميات غذائية بمعرفة عدد الخطوات التي مشوها ومدى نشاطهم بدقة، عبر تأمين معلومات يمكن قياسها وجمعها بواسطة أجهزة حاسب صغيرة يمكن ارتداؤها على الجسم. ويمكن

عرض هذه المعلومات على لوحات بيانية أنيقة التصميم على الحاسب، تصف بوضوح آخر صيحات اللياقة، حتى إنها تؤمن عناصر التلعيب مع لوائح بالمتصدرين وشارات تُمنح عند تحقيق الأهداف الموضوعة مسبقاً. ويمكن لمتبعي الحميات الغذائية أن يغيروا سلوكهم بأن يتناولوا كميات أقل وأن يتحركوا أكثر عند تزويدهم بهذه المعلومات لتحقيق الخسارة في الوزن التي يصبون إليها. وقد تؤدي هذه الأجهزة دوراً مهما في الوقاية من الأمراض وتحسين الصحة العامة.

تم بيع أكثر من 100مليون من الأجهزة القابلة للارتداء في أنحاء العالم عام 2014، ومن المتوقع أن تصل هذه المبيعات إلى 485 مليون وحدة بحلول عام 2018. ويمكن تصنيف الأجهزة القابلة للارتداء في تصنيفات واسعة، مثل أسورة تعقب النشاطات كـ فيتبيت.فليكس وجو.بونز.أب ونايكي.فيول.باند، والساعات الذكية (بيبل وسامسونغ غالاكسي جير، وساعة آبل الآتية قريباً)؛ وحتى النظارات مثل نظارات غوغل. وعلى الرغم من أن سوق الأجهزة القابلة للارتداء لا تزال سوقاً ضيقة حتى الآن، فإنها قادرة على التحول أجهزة رئيسية في المستقبل القريب.

يمكن مزامنة الأجهزة القابلة للارتداء مع الهاتف النقال الخاص بالمستخدم بوساطة الاتصال بالبلوتوث أو الوايفاي، وعندما يتم ذلك، ستنضم صحتك الشخصية لإنترنت الأشياء أيضاً، وستكون سهلة الاختراق كغيرها من أغراض إنترنت الأشياء. علاوة على ذلك، ترتبط العديد من الأجهزة القابلة للارتداء بشبكات التواصل اجتماعي، إذ يمكن لجهاز التعقب فيتبيت أن ينشر تلقائياً عدد الخطوات اليومية التي مشيتها على صفحتك في الفايسبوك على سبيل المثال. وهو ما يفرض طيفاً واسعاً من المخاوف المتعلقة بالخصوصية، وبالأخص حول هوية من يملك البيانات، وكيفية تأمينها، وكيفية مشاركتها مع أطراف أخرى. ومن المفاجئ على أية

حال أن 25% من تطبيقات اللياقة البدنية لا تمتلك أية سياسات متعلقة بالخصوصية. وكما تعلمنا، فإن المعلومات التي تبدو لك غير ضارة الآن قد تعود لتزعجك لاحقاً. فقد لأنماط النوم المضطربة التي يتم تسجيلها تلقائياً بوساطة جهازك القابل للارتداء فائدةٌ في قضية محكمة بشأن حادث سيارة. هل ستطلب منك شركة التأمين الصحي ارتداء جهاز تعقبٍ للنشاطات لكي تحصل على أفضل العروض كما تفعل شركات تأمين السيارات بصناديقها السوداء في سيارتك؟

إن إحدى أحدث الصيحات في عالم الحوسبة القابلة للارتداء هي دمج كاميرات فيديو داخل الأجهزة، سواء كانت كاميرا غو.برو.إتش.دي الشائعة والمزودة بتقنية وايفاي المستخدمة في تصوير النشاطات الضخمة، أو شيئاً أكثر دقة مثل الكاميرا المدمجة ضمن نظارات غوغل. قد تبدو فكرة تجول معظم الناس في شوارعنا وهم يرتدون نظارات مزودة بكاميرا فيديو متصلة بالإنترنت منافية للعقل في الوقت الحالي، لكن عليك أن تتذكر أن الكلام نفسه قيل عن الحاسب الشخصي والهاتف النقال. لقد وقّعت غوغل بالفعل عقد شراكة مع شركة النظارات الضخمة لوكسوتيكا، لدمج نظارة غوغل مع نظارات "وكليز وراي.بان"، كما تنبأت شركة ديلويت ببيع ملايين النظارات الذكية في عام 2015. وستؤمن أجهزة مثل نظارات غوغل قدراً كبيراً من الرفاه التقني مدمجاً في جهازٍ واحد محمول، كالقدرة على التقاط الصور وإرسالها وتسجيل الفيديو وإجراء المكالمات الهاتفية والبحث على الإنترنت وإرسال الرسائل النصية القصيرة وقراءة البريد الإلكتروني. هذه القدرات هي ذروة ما يمكن القيام به اليوم في سوق الحوسبة القابلة للارتداء، وسيتم تعزيزها عبر ربطها بمجموعة متنوعة من تقنيات الاتصال بالبلوتوث والوايفاي والجي.بي.إس، إلى جانب ربطها بما يتلاءم مع خطط البيانات المحمولة على هواتفنا الذكية. وكما نوهنا في فصول سابقة، بناءً

على ملاحظات السيد بورنز من مسلسل سيمبسونز والسيد شيرتوف من وزارة الداخلية، فإن كل القوة وإمكانات الاتصال التي تتيحها نظارات غوغل، ستترافق مع مجموعة من قضايا سياسات الخصوصية والسياسات العامة. ولكن هناك تهديدات أمنية هامة يجب أخذها في الاعتبار أيضاً.

لقد أدى الخوف من التصوير لحظر نظارات غوغل في العديد من الأماكن العامة، من ضمنها المناسبات الرياضية والحفلات الموسيقية وغرف تبديل الملابس في النوادي الرياضية، والبارات والمطاعم ونوادي التعري والكازينوهات والمشافي وصالات السينما البريطانية. وتتضمن الأسباب المطروحة لمنع هذا الجهاز كل شيء، بدءاً من ألعاب الورق إلى قرصنة الأفلام والتجسس الصناعي. ولكن ثمة مخاوف أخرى بعد، فمن الممكن اختراق نظارات غوغل لالتقاط الصور وتسجيل الفيديو بشكلٍ سري، ليتم إرسال البيانات خلسةً إلى شركة الجريمة في أي مكان في العالم وبدون علم مالك الجهاز. كما حدث تماماً مع البرمجية الخبيثة التي يتم استخدامها لتخريب حاسبك الشخصي أو هاتفك النقال، يمكن تشغيل نظارات إنترنت الأشياء بدون دليل مرئي على أنها تسجل.

لقد كسر المخترقون بالفعل أمن نظارات غوغل حتى قبل عرض الجهاز للبيع لعامة الناس. ووجود ثغرات أمنية في نظارات غوغل يعني أنه يمكن تجميد الجهاز وتخريبه لنقل كل ما تسمعه وتراه بالزمن الحقيقي، بما في ذلك تفاصيل حساباتك وكلمات السر التي تقوم بإدخالها لتسجيل الدخول لحسابك المصرفي على الإنترنت. كما أن خواص نظام جي.بي.إس في النظارة ستسمح لشركة الجريمة بتحديد مكانك بدقة، كأن تكون مثلا أمام صرافٍ آلي تقوم بكتابة رقم التعريف الشخصي. وبينما لم تكن جدتك بحاجة لبرنامج مضاد للفيروسات من أجل نظاراتها، قد تكون أنت بحاجه له. فقد تم بالفعل إنشاء العديد من البرمجيات الخبيثة وأدوات التجسس

المخصصة لنظارات غوغل. نتيجة لذلك، بات من الممكن اليوم، ولأول مرة في تاريخ البشرية، اختراق كرتي عينيك أيضاً.

نظراً لسرعة التقدم التقاني، فإن ارتداء جهاز حاسب "ضخم" داخل نظاراتنا سيصبح أمراً صعباً على الجيل القادم، ومن المؤكد أن الدورة الجديدة لهذه الأجهزة ستتمثل في تزويد العدسات اللاصقة بإمكانية الاتصال بالإنترنت. وبينما لا يزال على غوغل أن تؤكد رسمياً وجود نسخة مخصصة للعدسات اللاصقة من نظارات غوغل، فإنها فاجأت العالم في منتصف عام 2014 عندما أعلنت أنها تعمل على مشروع "عدسات لاصقة ذكية" لإنترنت الأشياء، بالتعاون مع شركة نوفارتيس الدوائية. وستوفر العدسات التي تنتجها هذه الشركة مجموعةً من الشرائح الصغيرة لحساسات وهوائيات ستجعل مراقبة مستوى سكر الدم لدى مرضى السكري باستمرار أمراً ممكناً، ولأول مرة في التاريخ بدون الحاجة لوخزات الإبر المؤلمة التي تتطلبها أنظمة فحص مستوى الغلوكوز الحالية. لا يزال الجهاز في مراحل الاختبار الأولى بالتعاون مع إدارة الأغذية والعقاقير (إف.دي.أي). كما تعمل سامسونغ الآن، لكي تواكب التطورات، على تطوير عدسات لاصقة كاملة التجهيز ومتصلة بالإنترنت، ستتمكن من عرض كافة البيانات الشبكية المتاحة حالياً في نظارات غوغل ولكن على شكل عدساتٍ لاصقة باستخدام صمامات ثنائية باعثة للضوء مدمجة فيها وخليط من الأسلاك النانوية المصنوعة من الغرافين والفضة. ولكن حتى تصل الأجهزة القابلة للارتداء إلى التطور الذي تعدنا به وتتمكن من دمج الإنسان بالآلة بشكلٍ كامل، لا يزال هناك حدّ أخير يجب تجاوزه: زرع الحواسب داخل الجسم نفسه.

أنت تحطم قلبي: أخطار الحواسب القابلة للزرع

كانت المرة الأولى التي يتم فيها زرع جهاز طبي إلكتروني بنجاح في الجسد

الإنساني عام 1958. وقد أجرى العملية الجراحية البطولية جراحان سويديان للمهندس آرني لارسن الذي عاش ثلاثاً وأربعين سنةً بعد ذلك، حياة كاملة من الذكريات والتجارب لم يكن ليعيشها لولا الحاسب الذي يعادل حجمه حجم قرص لعبة الهوكي، والذي تم تركيبه في تجويف البطن ليجعل قلبة يدقُّ بانتظام. والآن، بعد نحو ستين سنة، تم تحقيق قفزات مدهشة في عالم الطب عبر تطوير قدرات وحجم الأجهزة الطبية القابلة للزرع. فقد شهدت هذه الأجهزة تحسناً في العديد من جوانبها، كقابلية النقل وعمر البطارية والفعالية، وبات يمكنها اليوم تحويل المعلومات الهامة إلى الطبيب عبر الإنترنت. فقد تم زرع أول جهاز لتنظيم ضربات القلب مزود بالوايفاي في الولايات المتحدة في صدر كارول كازيجانسكي من مدينة روزلين في نيويورك عام 2009، وعند انتهاء العملية الجراحية، كان قلبها النابض أول قلبٍ ينضم لإنترنت الأشياء.

إلى جانب أجهزة تنظيم ضربات القلب، بات الكثير من الأجهزة القابلة للزرع شائع الاستخدام في أنحاء العالم اليوم، منها مزيلات الرجفان ومضخات الإنسولين الخاصة بمرضى السكري وقوقعة الأذن المزروعة والمحفزات العصبية. وبينما يملك كل جهاز أهدافه العلاجية ضمن الجسم، تتواصل الأجهزة القابلة للزرع مع العالم الخارجي عبر بروتوكولات الموجات الراديوية المعروفة مثل البلوتوث والوايفاي والاتصال القريب المدى (إن.إف.سي) والمعرف الترددي الراديوي (آر.إف.آي.دي). وتم تزويد ملايين الأميركيين بأجهزة قابلة للزرع، إذ يتلقى نحو 300,000 مريض أجهزةً طبية لاسلكية قابلة للزرع كل سنة. وقد انتشرت هذه الأجهزة بشكلٍ كبير في عالم الطب الحديث، نظراً لصغر حجمها وإمكاناتها المتزايدة والفوائد الطبية الجلية التي تقدمها. إذ تسمح الأجهزة الطبية اللاسلكية، مثل مقوم نظم القلب مزيل الرجفان القابل للزرع (آي.سي.دي)، للأطباء بمراقبة ضربات

قلب المريض عن بعد والحصول على تخطيط لكهربية القلب بشكلٍ فوري، ما يخفف الحاجة لزيارات العيادة العالية التكلفة. وفي حال تم الكشف عن وجود مشكلة عبر جهاز آي.سي.دي، يمكن للأطباء أن يتصلوا بالمرضى مباشرةً وليعلموهم بحاجتهم لإجراء زيارة والخضوع للعلاج. لا يمكن المبالغة بوصف القدرات الكبيرة التي تمتاز بها هذه الأجهزة في إنقاذ حياة المرضى، ولكن مع تزايد دمجنا لتقانة المعلومات في البيولوجيا الخاصة بنا، سينضم المزيد من الناس لأمة السايبورغ، مع مضاعفات خطيرة على سلامتهم وخصوصيتهم وأمنهم.

تمثل أعطال الأجهزة الطبية المتعددة المهام أحد أهم أسباب الإصابات الخطيرة والوفاة في الولايات المتحدة، كما أن عدد حالات سحب الجهاز تضاعفت بين عامي 2004 و2014، وكان السبب وراء ما يقارب 25 بالمئة من حالات سحب الأجهزة هو وجود عطل متعلق بالحاسب، فقد كانت 94% من هذه الحالات "تفرض خطر حدوث مضاعفات صحية بالغة بدرجة تتراوح بين المتوسطة والعالية". حتى ضمن المستشفيات، وُجِدَ أن معظم الأجهزة العلاجية، مثل التصوير بالرنين المغناطيسي والأشعة السينية وآلات التخدير ومضخات التسريب وأجهزة التصوير المقطعي المحوسب وأجهزة التنفس الاصطناعي مليئة بفيروسات الحاسب، ويمكن للمخترقين استغلالها عن بعد بيسر. وقد أطلقت وزارة الداخلية عام 2013 بالفعل تحذيراً موجهاً للمرافق الطبية، تشير فيه إلى وجود أكثر من ثلاثمئة جهاز من أربعين شركة مختلفة تحتوي على نقاط ضعفٍ يمكن استغلالها بسهولة من قبل أصحاب الغايات المريضة. يبدو أن الأجهزة الطبية التي تعتمد عليها حياتك قد تنهار مثل نظام ويندوز في الحواسب. وثمة فرق كبير على أي حال بالنسبة للأجهزة القابلة للارتداء. فعلى عكس هاتفك الذكي، لا يمكنك ببساطة أن تحمّل برمجيات ثابتة جديدة لجهاز تنظيم ضربات القلب عبر

الهواء. بدلاً من ذلك، على الجراحين أن يشقوا صدرك أو بطنك ليتمكنوا من الوصول للجهاز لإجراء تحديث كامل للبرنامج الثابت أو استبدال الجهاز.

ربما يكون مصدر القلق الأكبر هو كلما زرعنا أجهزة حاسب صغيرة داخلنا بهدف مراقبة وتحسين صحتنا، خلقنا فرصاً للآخرين لاختراق أجسادنا والقيام بتخريب هذه الآلات لغاياتٍ شريرة. إذ يتم بيع العديد من الأجهزة الطبية بدون وجود أي آليةٍ أمنية. حيث يميل مصنعو الأجهزة القابلة للارتداء بدلاً من ذلك إلى الاعتماد على "أمان المُغْفَل". ففي النهاية، لِمَ سيفكر أي شخص باختراق جهاز لتنظيم ضربات القلب؟ يهمل هذا المنطق الخطأ حقيقة الوجود الفعلي لأقلية صغيرة من الناس القاسية والبغيضة في العالم ستكون سعيدة بالحصول على فرصة لإثبات مهاراتها التقنية على حساب الآخرين. وقد حدث هذا عندما قام المخترقون عام 2008 بتبديل موقع الويب الخاص بمنظمة الصرع الوطنية، ليضموا إليه مئات الصور المتحركة سريعة الوميض، ما سبب نوبات عنيفة بين مرضى الصرع الذين كانوا يقومون بزيارة بريئة للموقع بغرض الحصول على المشورة الطبية.

بيّن فريقٌ من الباحثين من جامعتي ماساتشوستس وواشنطن، أن هذا الخطر قائم فعلاً عندما نجحوا في اختراق الأمن اللاسلكي لجهاز ميدترونيك، الذي يجمع بين مزيل الرجفان ومنظم ضربات القلب. فبعد التمكن من الدخول غير المشروع للجهاز، تمكنوا لا فقط من قراءة معلومات المرضى السرية، بل كان الأسوأ هو أنهم استطاعوا أن يرسلوا صدمات كهربائية للقلب الذي يعمل بشكلٍ طبيعي، وهو فعلٌ قد يقتل شخصاً بريئاً سيئ الحظ. تمثل الأجهزة القابلة للارتداء بالنسبة للمخترقين طريقة جديدة لا يمكن مقاومة إغرائها لقياس مهاراتهم، ويعد هذا الموضوع أحد أكثر المواضيع شهرةً في مؤتمر بلاك هات السنوي في لاس فيغاس. فقد نجح أحد المخترقين المعروفين، وهو بارنابي جاك، بتخريب عددٍ من أجهزة إنترنت

الأشياء، بدءاً بالصرافات الآلية وانتهاءً بأجهزة تنظيم ضربات القلب. فقد اكتشف جاك عام 2012 عيوباً برمجية خطيرة في الأجهزة القابلة للارتداء التي ينتجها بعض المصنِّعين، تسمح بالسيطرة على هذه الأجهزة. فعن بعد خمسين قدماً، وباستخدام حاسب شخصي فقط، تمكن المخترق من أمر جهاز مزروع بتوصيل شحنة شدتها 830 فولت مباشرةً إلى القلب، وهي شحنةٌ من القوة بما يمكنها بالتأكيد قتل أي شخص لديه جهاز تنظيم ضربات القلب مزروع داخله.

خوفاً من وقوع هجوم كهذا، قام اختصاصي الأمراض القلبية الخاص بنائب الرئيس الأميركي السابق ديك تشيني، بتغيير جهاز آي.سي.دي الخاص بنائب الرئيس بإزالة الميزات اللاسلكية، خشية أن يقوم الإرهابيون بالفعل بإرسال صدمات كهربائية قاتلة لقلبٍ مريضٍ يكاد يكون القائد الأعلى للدولة. وفي إحدى التجارب التي يحاكي فيها الفن الحياة، تم تصوير نسخة خيالية، ولكن قابلة تماماً للتطبيق، لمثل هذا الهجوم في مسلسل هوملاند الدرامي الحائز جائزة إيمي. حيث يدير الإرهابي الشرير "أبو نظير" عملية اغتيال نائب الرئيس عبر الإنترنت عبر إضعاف جهاز الآي.سي.دي إلى حدّ مميت. لكن أجهزة تنظيم ضربات القلب ليست الأجهزة الوحيدة القابلة للارتداء التي تمكّن منها القراصنة. فمئات الآلاف من المواطنين في الولايات المتحدة يعتمدون على مضخات الأنسولين الخاصة بمرضى السكري أيضاً. والغاية من هذا الجهاز هي إفراز الأنسولين بكمياتٍ مضبوطة بدقة لمن يحتاج لضبط مستوى السكر في دمه. ومرة أخرى، أثبت السيد جاك الموهوب قدراته وخبراته التقنية، وهزم النظام الأمني الضعيف في بعض مضخات الأنسولين الشائعة في السوق. فقد كان جاك قادراً على تحديد موقع أية مضخة أنسولين ضمن دائرة نصف قطرها ثلاثمئة قدم وتخريب هذه المضخات باستخدام هوائي راديوي مُخصص قام هو بصنعه، ما أدى

لإطلاق كمية الأنسولين المخصصة لخمسةٍ وأربعين يوماً بشكلٍ فوري مرةً واحدة، في هجوم افتراضي سيؤدي، إلى حد شبه مؤكد، إلى الموت إذا لم تتوفر مساعدة طبية فورية.

ربما لم تُكشف أية هجمات إجرامية تستهدف الأجهزة القابلة للزرع حتى يومنا هذا، لكن يمكننا أن نتوقع من شركة الجريمة أن تولي اهتمامها لهذه الأجهزة. وقد تنبأت وكالة الشرطة الأوروبية، اليوروبول، بالفعل بأن تصبح جرائم القتل عبر الإنترنت من خلال الأجهزة القابلة للزرع حقيقة قائمة في بداية عام 2014. وقد تكون بعض هذه الحوادث مجرد هجماتٍ افتراضية تافهة، فمثلما يمكن لهجوم مبرمج من شبكة روبوتية (بوت.نيت) أن يسيطر على حاسبك وهاتفك النقال (وحتى برادك كما رأينا في الفصل السابق)، كذلك الأمر بالنسبة لجهاز تنظيم ضربات القلب. فالأجهزة الطبية المُخترقة تبدو كأي عنوان إنترنت متاح على إنترنت الأشياء، حالما يتعرض جهاز مزيل الرجفان أو مضخات الأنسولين للإصابة، يمكن للرسائل الضارة التي تم التلاعب بالجهاز ليرسلها أن تستهلك عمر البطارية المحدود، والثمين جداً، الضروري جداً لتنظيم ضربات القلب أو جرعات الأنسولين، ما سيتطلب تدخلاً جراحياً لاستبدال الجهاز.

من نافل القول أن عدد المؤامرات الشريرة الممكنة سيزداد مع تضاعف عدد الأجهزة الطبية المتصلة بالإنترنت. وستكون هناك في الواقع طرق جديدة لارتكاب جرائم القتل عن بعد عبر اختراق الأجهزة الطبية غير الآمنة، ما يدخلنا في الحقبة الكريهة للجرائم الطبية الافتراضية. فربما لن يصدر عن الحاسب الشخصي وميض الطلقة الذي يصدر عن فوهة المسدس، ولكن يمكن للأجهزة في عالمنا الحديث أن تقتل بالقوة نفسها. وستبحث شركة الجريمة عن طرق لتحويل الهجمات على الأجهزة القابلة للارتداء إلى نقود. فمثلما تقوم برامج الفدية كبرنامج كريبتولوكر بتخريب القرص

الصلب لحاسبك أو لهاتفك النقال لتجعله غير قابلٍ للاستخدام، لسنا نجافي المنطق حين نتوقع محاولات ابتزاز مشابهة بوساطة الأجهزة الطبية. "لديك ستون دقيقة لتحويل 10,000 دولار كعملات رقمية لهذا الحساب أو سنرسل صدمة كهربائية شدتها 830 فولت إلى قلبك"، ثم تأتي اللازمة "تيك توك، تيك توك...". والأسوأ من ذلك ما قد يحدث إذا استطاع المخترقون التسلل إلى أنظمة التحكم الصناعية في المعامل التي يتم فيها تصنيع أجهزة إزالة الرجفان القابلة للزرع وإدخال برمجيات اليوم صفر إليها. وقد لا يمكن ملاحظة التغييرات الدقيقة في البرمجية لأشهر أو سنوات بعد أن تكون مئات الآلاف من الأجهزة قد زُرعت لدى المرضى في أنحاء العالم. وعندها فقط قد تضرب شركة الجريمة ضربتها الأولى الحاسمة التي ستكون أول هجوم يستهدف البنى التحتية الهامة، باستخدام تقانة المعلومات بغرض مهاجمة البيولوجيا البشرية، مطالبةً بملايين الدولارات كفدية لتفادي أزمة عالمية. ولن يكون من الممكن معالجة آلاف وآلاف الأفراد ممن يحملون القنبلة الموقوتة في صدورهم في وقتٍ معقول، ما لا يترك خياراً سوى الاستجابة للمطالب.

نظراً للوتيرة التي يمليها قانون مور، علينا بلا شك توقع تقلص حجم الأجهزة الطبية القابلة للزرع وتعاظم قدرتها في تقديم فوائد طبية مميزة للمرضى. فقد ابتكر مهندسو الطب الحيوي في جماعة ستانفورد على سبيل المثال، جهاز روبوت لاسلكياً لا يحتاج لبطارية، وهو صغير جداً بحيث يمكنه أن يسبح في مجرى الدم ليقوم بالتشخيص وحتى بالعمليات الجراحية الدقيقة. إنها بشائر عالم ستار تريك الطبي. ولكن حتى هذه العلاجات العجائبية قد تكون عرضة لتهديداتٍ القراصنة، فقد يتمكنوا من التلاعب بالنتائج التي تقدمها هذه الأجهزة بحيث يتم إطلاق الأدوية في مجرى الدم بدون وجود الحاجة لذلك، أو أن يجعلوا الروبوت الدقيق

يهاجم النسج السليمة بدلاً من الأورام في حالات السرطان. فكيف لنا أن علم في حال تم اختراق الحواسب القابلة للبلع أو الحقن؟ ما هي الأدلة الباقية التي يمكن كشفها إن وُجدت؟

عندما يموت شخص يحمل جهازاً قابلاً للزرع، ستواجه الكادر الطبي الموكل إليه تحديد سبب الوفاة عدة أسئلة: هل كان هذا موتاً عرضياً ناتجاً عن خطأ في وظيفة الجهاز القابل للزرع؟ هل وقع الجهاز ضحية لهجومٍ إجرامي؟ أو هل كان هذا انتحاراً قام به المريض بنفسه عبر تخريب جهازه القابل للزرع لإنهاء معاناته وأمله آملاً أن تحصل عائلته على أموال التأمين على حياته نتيجة موته الطبيعي ظاهرياً؟ بينما يتطور الطب الحديث ويزداد عدد الأجهزة القابلة للزرع، تنبغي الإجابة على سؤالٍ حيوي: عندما يوجد جسدٌ متطور تقانةً في المشرحة، من سيكون قادراً على تشريح الجثة؟ من المؤكد أن الأطباء وعلماء الطب الشرعي لا يملكون أي تدريب على الطب الشرعي المحوسب. كيف إذاً سيمكنهم تحديد سبب الوفاة؟ لن يتمكنوا من ذلك، كما أن التهديد الذي يفرضه انعدام أمن الأجهزة الطبية يجعل الفرار بعد ارتكاب جريمة قتل أسهل.

عندما يصاب ستيف أوستن وجايمي سمرز بفيروس

يربط الهاتف الذكي بين أجساد المرضى وحواسب الأطباء التي تتصل بدورها بالإنترنت التي تتصل بدورها أيضاً بأي هاتفٍ ذكي في أي مكان. يمكن لهذه الأجهزة أن تضع إدارة أعضاء الأفراد الداخلية بين يدي أي مخترق أو مخادع على الإنترنت أو مخربٍ رقمي على كوكب الأرض.

تشارز سي.مان

بعد فترة قصيرة على وقوع مشاهدي التلفاز في السبعينيات في حب ستيف أوستن، النجم ورائد الفضاء المُعاد بناؤه في مسلسل "رجل الستة ملايين دولار"، أصبحت برفقته أنثى اسمها جايمي سمرز كانت أول امرأة

بأعضاء آلية في العالم. ومع أن الاثنين واجها وهزما الكثير من الأشرار، فإن أحداً لم يحاول التصدي للبطلين الخارقين عبر تخريب الإلكترونيات الموجودة في أعضائهما الآلية. لم لا؟ ربما لأن فيروسات الحاسب والتقنيات اللاسلكية لم تكونا من روح ذلك العصر، ولكن كما رأينا مع بيرتولت ماير، فإنه عندما يمكن التحكم لاسلكياً وعبر الإنترنت بيدك أو رجلك أو ذراعك، فإنه من الممكن أن يتم استهدافها من قبل المخترقين كأي غرض في إنترنت الأشياء. مع أنها الآن غير شائعة نسبياً، فإن استخدام تعويضات الأطراف سيشهد زيادة هائلة في السنوات القادمة، مدفوعاً بالأخص بحاجات آلاف الجنود الشبان العائدين من العراق وأفغانستان والذين تعرضوا لإصابات خطيرة خلال الحرب.

استجابةً لذلك، أطلق البنتاغون مع وكالة مشاريع البحوث المتطورة الدفاعية، داربا، برنامجاً ثورياً للأطراف الصناعية باستثمارٍ بلغ 100 مليون دولار، وباشتراك أكثر من ثلاثمئة عالمٍ بهدف تغيير عالم الأطراف الآلية تغييراً جذرياً. كان أحد نجاحات هذا المشروع هو الذراع الصناعية "لوك آرم/ ديكا" التي ابتكرها دين كامين، والتي استوحي اسمها من الذراع الآلية لـ "لوك سكاي واكر" من فيلم حرب النجوم. ويتم التحكم بالجهاز عبر إشارات كهربائية يتم إرسالها من أقطاب متصلة بعضلات الإنسان، وهي دقيقة لدرجة أن أصابعها يمكنها التقاط ربع دولار تم إلقاؤه بشكلٍ أفقي على طاولة. وثمة جهود أخرى ما زالت مستمرة أيضاً، ومن بينها مشروع الأطراف الآلية البشرية في معهد ماساتشوستس للتقانة، والذي يحتوي على "مخزن لمبتوري الأطراف يحتوي على جميع الأطراف التعويضية التي حازت موافقة إدارة الأغذية والعقاقير، ما يسهل عليهم إيجاد أسهل الطرق لإعادة بناء أجسادهم". لقد تم ابتكار أعضاء آلية يمكن زرعها مثل البنكرياس لمساعدة مرضى السكري على تنظيم مستويات السكر لديهم، ويمكن

التحكم به بأريحية عبر تطبيقٍ على هواتفهم الذكية يتصل لاسلكياً بالعضو الآلي.

ثمة مجالٌ آخر في عالم الأطراف الآلية يتطور بسرعة، وهو تسويق الهياكل الخارجية أو الروبوتات القابلة للارتداء مثل نظام "إيكسو بيونيكس" الذي يسمح عند ارتدائه خارجياً للمشلولين بسبب السكتات الدماغية أو إصابات العمود الفقري أو المرض بالسير من جديد. وتدعم بدلة الهيكل الخارجي هؤلاء الذين لا يمكنهم المشي، فتحرك أطرافهم بدلاً منهم في الحقيقة، وتسمح لهم أن يقفوا ويتحركوا بلطف. ويمكن للأشخاص الذين يعانون إعاقات جسدية استخدام تصاميم إيكسو التي تؤمن مساعدةً وقوة كبيرة بتخفيف العبء على العضلات السليمة، ما يسمح للجنود، على سبيل المثال، بحمل مئات الأرطال لمسافاتٍ بعيدة دون تعب. كما طور طلاب التخرج في برنامج جامعة نيويورك للاتصال السلكي واللاسلكي التفاعلي "واجهة برمجة تطبيقات مفتوحة المصدر تسمح لك بتحريك ذراع شخصٍ آخر عن بعد باستخدام لوحة مفاتيح أو عصا للتحكم أو حتى هاتف آيفون"، لمساعدة المشلولين أو الأشخاص غير القادرين على التحكم بأطرافهم بشكلٍ كامل على تحريك أطرافهم بشكلٍ طبيعي. والنتيجة هي السيطرة غير الذاتية على الجسد عبر السماح للآخرين بالتحكم بذراعك أو رجلك عبر الإنترنت.

لن يقتصر مستقبل الأعضاء الآلية بالطبع على استعادة القدرات البشرية المفقودة بسبب الإصابة أو المرض. إذ تتركز الفرص التسويقية الكبرى على تحسين القدرات البشرية، بما يمنحنا قوى لم نملكها يوماً ويزيد القوى التي لدينا بالأصل. فمن منا لا يرغب بالحصول على القوى البشرية الخارقة التي جسدها طوني ستارك في فيلم الرجل الحديدي؟ لكن قدرتنا المتزايدة على تحويل الجسم الإنساني عبر تحسين البيولوجيا الخاصة بنا بوساطة تقانة

المعلومات، تترافق مع مجموعة من المخاطر والأسئلة الأخلاقية الواجب مواجهتها في المستقبل. فمن الممكن بلا شك أن تصاب رجلاك الآليتان بفيروس أو أن تُخترف يدك الآلية، ولكن ماذا سيحدث عندما تصبح الهياكل الخارجية الآلية متوفرة للإنسان العادي ويبدأ المحتالون باستخدام القوة البشرية الخارقة لسرقة الآخرين؟ تخيل مستقبل حرب الشوارع بين العصابات عندما يمكن لعصابتي جريبس وبلودس أن تحصلا على هذه الأدوات لتبدآ التعارك بها في شوارع مدينتك، أو أن ترسل شركة الجريمة رجلاً يرتدي هيكلاً خارجياً يطرق بابك ليجمع دين القمار الذي عليك أن تدفعه. قد تبدو هذه السيناريوهات خيالية، إلا أن تاريخاً طويلاً من التقانة العسكرية يتبناه العامة في النهاية، سواء تمثل في الأسلحة النارية أم في مناظير الرؤية الليلية أو الملاحة بواسطة الجي.بي.إس أو حتى الإنترنت. فمن الواضح أن طرقاً عديدة ستتاح في المستقبل للمخترقين، ستسمح لهم بالاستفادة من التطورات الحالية والقادمة في مجال الحوسبة القابلة للزرع أو الارتداء. ولكن ثمة طرق أخرى لاستخدام البيولوجيا البشرية كالأمن والتعرف على الهوية، وهنا ستكون أرض المعركة للسيطرة على أجسادنا وعلى ذواتنا.

أزمة الهوية: اختراق القياسات الحيوية

عادةً ما نميل للاعتقاد بأن وجوهنا وعيوننا وأصواتنا وأصابعنا وضربات قلبنا وأرجلنا وراحت أيدينا، هي عناصر فريدة في علم الأحياء والتشريح تنتمي لنا ولنا وحدنا من دون شك. ليت هذا يكون صحيحاً. فنحن نشارك كمية متزايدة من المعلومات حول صفاتنا الجسدية والسلوكية مع الآخرين، سواء أدركنا ذلك أن لا أم. تمثّل هذه المعرِّفات البيومترية صفات جسدية مميِّزة، وأكثرها شيوعاً هي بصمات الأصابع التي استخدمتها الشرطة لأكثر من 125 سنة للتعرف على المجرمين.

على مدى أكثر من قرن، كان تحليل بصمات الأصابع يتم بشكلٍ يدويٍّ فقط من قبل تقنيين مدربين تدريباً خاصاً. لكن الأمور على كل حال تغيرت، فالتطورات السريعة في طاقة معالجة البيانات وتقانة أجهزة الاستشعار جعلت الحواسب بدورها قادرة على إجراء عملية التعرف على الهوية بواسطة القياسات الحيوية. نتيجة لهذا، يتزايد انتشار أنظمة القياس الحيوي لتصبح مع الوقت أكثر شيوعاً في حياتنا اليومية. وستخلق أنظمة القياس الحيوي نقلةً كبيرة في طريقة التعرف على هويتنا في المستقبل. فعلى عكس الوسائل التقليدية لتحديد الهوية، حيث كنت بحاجة لحمل شيءٍ معك كشهادة القيادة أو جواز السفر، أو تذكر شيءٍ ما مثل كلمة السر أو رقم التعريف الشخصي، نظم القياسات الحيوية هي شيء موجود دائماً معك وليس عليك الخوف من نسيانه. فالنظم البيومترية هي أنت.

تستخدم النظم البيومترية لتحديد الهوية حساسات حاسوبية لقياس أشياء كالنتوءات في بصمات أصابعك والمسافات بين ملامح وجهك ونبرة ونوعية صوتك. وتتم ترجمة كل هذه المعلومات إلى أصفار وواحدات يمكن مقارنتها وحفظها وإعادة التعرف عليها، بحيث يمكن مطابقة بصمات أصابعك بدقة مع قاعدة من البيانات التي تعود لمئات ملايين الأشخاص في غضون ثوانٍ. ونظراً لكلفتها المنخفضة وقدراتها المتزايدة، من المتوقع أن تنمو سوق أنظمة القياسات الحيوية العالمية لتصل قيمتها إلى 23 مليار دولار بحلول عام 2019، مع أكثر من 500 مليون حساس بيومتري ستنضم لإنترنت الأشياء بحلول عام 2018. ستصبح أنظمة القياس الحيوي ضخمة، وستكون في كل مكان، وقد بدأت بذلك بالفعل.

يُطلب من مرتادي النوادي الرياضية أن يستخدموا بصمات أصابعهم في نوادي اللياقة البدنية المفتوحة على مدار الساعة. ولم يعد مطلوباً من المرضى في المركز الطبي التابع لجامعة نيويورك إحضار بطاقات التأمين

الصحي بعد الآن، لأن المشفى أدخل أكثر من 125,000 شخص في نظام بيشنت سيكيور الخاص به، إذ يستخدم هذا النظام ماسحاً ضوئياً بيومترياً متخصصاً في قياس أنماط توزع الأوردة الفريدة الموجودة في راحة اليد، كوسيلة أساسية في التعرف على المرضى. ولكن إذا كانت المشافي عاجزة عن تحصين أجهزة التصوير بالرنين المغناطيسي من البرمجيات الخبيثة، كيف ستنجح في حماية معلوماتك البيومترية؟ وهل ترى أنها فكرة جيدة أن يتمكن أفراد طاقم النادي المحلي الرياضي الذي ترتاده (والذين غالباً ما لا يملكون أية خبرة في مجال الأمن البيومتري) من الوصول لبصمات أصابعك؟

تبدو الماسحات الضوئية البيومترية التي نراها في أفلام التشويق الجاسوسية الهوليوودية، مثل فيلم مهمة مستحيلة، على قدر عالٍ من التقنية والقدرة، فماسحات العين الضوئية وقارئات بصمات الأصابع وأنظمة التعرف على الوجه تميّز الصديق من العدو بشكلٍ مثالي. مع مثل هذا التسويق، من السهل أن نفهم السبب وراء اعتقاد الناس بأن أنظمة التعريف البيومترية لا يمكن هزيمتها. لكن ما يتضح هو أن الأنظمة البيومترية ليست آمنة أو لا يمكن خداعها كما كان يعتقد في معظم الأحيان، وقد خلص تقرير لمجلس الأبحاث الوطني تم إعداده عام 2010 إلى أن هذه الأنظمة "عرضة للخطأ بطبيعتها". حيث يمكن لا نسخ العلامات الحيوية وحسب، بل إن قاعدة البيانات التي تخزن فيها كافة المعلومات البيومترية (التمثيلات الرقمية لعينيك ووجهك وأصابعك)، هي عرضة للاختراق ككل أنظمة المعلومات. وبعيداً من هذه المخاطر، فإن كلاً من الحكومات والقطاع الخاص يتسابقان لنيل أي ميزة أمنية ممكنة أو عائد اقتصادي من جمع تفاصيلك البيومترية، والتي يمكن جمعها بدون إذنك أو معرفتك.

تدير الحكومة الهندية أكبر قاعدة بيانات حكومية للهويات البيومترية في

العالم. ويعد المشروع، المعروف باسم أدهار (أي "مؤسسة")، محاولةً طموحة لتوثيق بصمات الأصابع والصور الشخصية وإجراء مسح ضوئي لقزحية عين المواطنين البالغ عددهم 1.2 مليار. وقد تَسلَّم ما يفوق 500 مليون مواطن هندي أرقام التعريف الخاصة بهم من "أدهار"، وخزِّنت معلوماتهم البيومترية في قاعدة البيانات الوطنية. ولكي تواكب الحكومة الأميركية هذه التطورات، فإنها كرَّست موارد مالية ضخمة لوزارة الداخلية ووزارة الدفاع ووزارة العدل، لتؤسس كل منها برامج بيومترية ضخمة في عالم ما بعد 9/11.

بينما قد تبدو قاعدة بيانات حكومية كهذه مفيدة في القبض على المجرمين والإرهابيين، فإن الأمر لا يخلو من المخاطر الأمنية وتلك المتعلقة بالخصوصية. فكما اكتشفت الحكومة الإسرائيلية عام 2011، فقد أعلنت سلطات البلد الشرق أوسطي أن قاعدة البيانات البيومترية الخاصة بها قد سرقت بأكملها، بما في ذلك الأسماء وتواريخ الميلاد وأرقام الضمان الاجتماعي والأرقام العائلية وتفاصيل حالات التبني، وتواريخ الهجرة والسجلات الطبية لتسعة ملايين إسرائيلي. وكان من سرق هذه المعلومات هو أحد المقاولين، لكنها بيعت بعد ذلك لشركة الجريمة وتم نشرها في النهاية كاملةً على الإنترنت في الأوساط السرية الرقمية. إن فرص الاحتيال وانتحال الشخصية بطرق متنوعة وغير ذلك من المشاكل الأمنية تبدو إذاً واضحة جداً.

تقدِّر شركة "جارتنر" أنه بحلول عام 2016 ستستخدم 30% من الشركات هويات بيومترية لموظفيها. إذ سيتم تضمين حساسات بيومترية في أرقى الهواتف المحمولة بنهاية عام 2015، ومن المقدر أنه بحلول عام 2018 سيصبح 3.4 مليون مستخدم للهواتف الذكية قادراً على فتح هاتفه ببصمات أصابعه أو وجهه أو عينيه أو صوته. فالأنظمة البيومترية هي

مستقبل الهوية والأمن ومنح التصاريح. وهي ستحل محل كلمة السر الشائعة الاستخدام التي يمكن اختراقها أو سرقتها بسهولة، كما أنها عاشت لفترة أطول بكثير من عمرها الوظيفي، كما ذكرنا مسبقاً في هذا الكتاب.

سيتيح الأمن البيومتري ميزاتٍ عديدة؛ فعندما تنسى كلمة السر أو رخصة القيادة، ستكون بصمات أصابعك معك دائماً. لكن إذا كانت الأنظمة البيومترية ستحل بعض المشاكل، فإنها ستخلق مشاكل أخرى. فمن الممكن اليوم، إذا كنت من بين عشرات ملايين ضحايا انتحال الهوية، أن تحصل على بطاقة ائتمان أو حتى رقم ضمان اجتماعي جديد. وإذا تم اختراق حسابك البنكي أو حساب الفايسبوك الخاص بك، يمكنك إعادة ضبط كلمة السر الخاصة بك. ولكن عندما تتم سرقة بصمات أصابعك، فلا توجد هنا إعادة ضبط. فهي علامات تعريفية دائمة، وحالما ينتزعها القراصنة ستصبح خارج نطاق سيطرتك، مرة وإلى الأبد. فعندما يملك كل من النادي الرياضي الذي ترتاده وشركة اتصالات هاتفك النقال وطبيبك كل معلوماتك البيومترية ويتم اختراق كل هذه الأنظمة، الأمر القادم لا محالة، ستكون معالجة المشكلة أكثر صعوبةً، إن لم تكن مستحيلة. فإذا كان مستقبل الهوية معتمداً بالكامل على النظم البيومترية، فسيشتمل مستقبل انتحال الشخصية على سرقة واختراق القياسات البيومترية، واللصوص والمحتالون يبذلون الجهود مسبقاً للتحايل على هذه الأنظمة.

الأصابع مشبوكة (ومخترقة)

إذا تم اختراق كلمة السر الخاصة بك، يمكنك تبديلها، كلما أردت ذلك. لكن لا يمكنك تغيير بصمات أصابعك. فلديك عشرة منها فقط، وأنت تتركها على كل شيءٍ تلمسه.

السيناتور آل فرانكين

تُعدُّ اللحظة التي قررت فيها شركة آبل إطلاق الإصدار الخامس من هاتف

آيفون الريادي في أواخر عام 2013 لحظة حاسمة في مجال نظم التعرف البيومتري على الهوية. إذ يمكن استخدام جهاز الاستشعار المدمج المعروف باسم تاتش.آي.دي لفتح الهاتف والقيام بعمليات الشراء على الإنترنت. وقد أتاحت آبل هذه التقانة للبائعين الآخرين، منذ بدئها باستخدام الإصدار الثامن من نظام آي.أو.إس، لتسمح لك باستخدام إصبعك بدلاً من تسجيل الدخول في الكثير من الخدمات والتطبيقات والأخرى. قد تبدو الراحة التي قد تنتج عن قدرتك على التعريف عن نفسك فوراً، بتمرير إصبعك والدخول بأمان لعدد ضخم من الخدمات على الإنترنت مغرية. وعلى غرار ذلك، أطلقت "سامسونغ" ماسحاً ضوئياً لبصمة الأصابع مع هاتف غالاكسي إس 5 المتطور، وكان الاختراق مصيره مثل هاتف آيفون. فقد أتاح الماسح الضوئي البيومتري في هاتف سامسونغ لمستخدميه إمكانية الاستعانة ببصمات أصابعهم للوصول إلى خدمات مثل حساب بايبال المخزن على الجهاز، أي إن اختراق بصمات الأصابع يمكن أن يؤدي لفتح المحفظة البيومترية والقيام بعمليات تحويل مالية غير مصرَّح بها لحسابات شركة الجريمة.

انخفضت كلفة حساسات بصمات الأصابع انخفاضاً ملحوظاً خلال السنوات العشر الماضية، حيث يمكن شراء بعض النماذج الرخيصة بنحو 10 دولارات. إن انخفاض سعر هذه الأجهزة يعني أن المزيد من المصنِّعين يقومون بدمج هذه التقنيات الأمنية في مجموعاتٍ متنوعة من الأجهزة، بما فيها الحواسب المحمولة. فسامسونغ وديل ولينوفو وسوني وإيسَر وأسوس، جميعها تشمل قارئات لبصمات الأصابع في حواسبها المحمولة، كما أنها شجعت المستخدمين على استخدام الأنظمة البيومترية لبصمات أصابعهم لقفل آلاتهم العاملة بنظام ويندوز، بل حتى في تشفير سواقات الأقراص الصلبة. الأمر عظيم من الناحية النظرية، لكن التطبيق كان سيئاً، وتمكن

المخترقون من رؤية التمثيلات الرقمية لبصمات الأصابع على شكل نصوصٍ عادية غير مشفَّرة، ما جعل كسرها أمراً سهلاً. توفّر جامعة الجريمة العشرات من الفيديوهات على الإنترنت، تشرح فيها كيفية اختراق الماسحات الضوئية لبصمات الأصابع، وقد تعلّمت شركة الجريمة منذ زمن طويل كيفية اختراق الأصابع، عبر قطعها. فقد استطاعت عصابات ماليزيا على سبيل المثال أن تتغلب على نظام تشغيل المحرك عن طريق تمييز بصمات الأصابع في سيارات مرسيدس إس.كلاس عبر قطع أصابع مالكي السيارات الفاخرة بالسكاكين. ومع أن مثل هذه الأعمال كانت شائعة في البرامج التلفزيونية مثل برنامج 24، فإن أيام قطع إصبع الخصم للدخول إلى مبنىً سري أو لجهاز حاسب لن تعود ضرورية بعد الآن. فقد ابتكر الباحث الأمني تسوتومو ماتسوموتو من جامعة يوكوهاما الوطنية طريقة تسمح له "بالتقاط صورة لبصمة خفية (على كأس نبيذ على سبيل المثال)" واسترجاعها عبر صك الجيلاتين. وهي تقنية جيدة بما يكفي لخداع الماسحات الضوئية البيومترية بنسبة 80% من المرات. وقد قام مخترقون آخرون باستخدام معجون تشكيل القوالب بلي - دو، الذي يعد لعبة شائعة للأطفال، لصنع قالب لبصمة الإصبع كان جيداً بما يكفي لخداع 90% من قارئات البصمات. وبينما يزداد انتشار الأنظمة البيومترية للتحكم بالوصول، ستزداد أيضاً دوافع التغلب عليها.

على الرغم من محاولات الحكومات والشركات إقناع العامة بالسلامة العالية والأمن الذي تقدمه الأنظمة البيومترية، يبقى الكثيرون غير مقتنعين، مظهرين قدراً كبيراً من المخاوف المتعلقة بالخصوصية ونقاط الضعف. وقد نشأ جدل علني في ألمانيا في عام 2008 عندما بدأ قائد شرطة البلاد ووزير الداخلية فولفغانغ شويبله بالترويج لنشر أنظمة بصمات الأصابع البيومترية. وكردٍّ على ذلك، استطاع الأصدقاء في نادي كاؤوس

للحاسب أن يرفعوا بصمات أصابع الوزير عن كأس ماء كان قد تركها وراءه بعد إلقاء كلمة في إحدى الجامعات المحلية. ونجح المخترقون بنسخ البصمة وأعادوا صنعها على شكل قالبٍ بلاستيكي، أربعة آلاف مرة. وتم توزيع البصمات المطابقة للأصل كهدية خاصة مرفقة بمجلة نادي المخترقين، إلى جانب مقالة تشجع القراء على استخدام البصمة وانتحال شخصية الوزير، ليفتحوا الباب أمام زرع بصماته في مسارح الجريمة.

يقول مناصرو الأمن البيومتري، إنه أكثر أماناً بطبيعته لأن أحداً لا يستطيع سرقة بصمات أصابعك (وهذا غير صحيح كما ذكرنا أعلاه)، ولأن بصمات الأصابع هي صفة مادية ثابتة لا يمكن تغييرها من قبل المجرمين. لكن تبين أن هذا غير صحيحٍ أيضاً، كما أثبتت المواطنة الصينية "لين رينغ" البالغة من العمر سبعةً وعشرين عاماً عام 2009. فقد دفعت لين للأطباء في الصين 14,600 دولار ليغيروا لها بصمات أصابعها، لكي تستطيع اجتياز الحساسات البيومترية التي تستخدمها سلطات الهجرة في مطارات اليابان. وكانت لين قد تم ترحيلها قبل ذلك، لكنها كانت مصرة على العودة إلى طوكيو، الأمر الذي لم يعد ممكناً بعد أن أعطت بصماتها الحقيقية عند وصولها إلى مطار ناريتا الدولي. فدفعت المال للجراحين الصينيين ليبدلوا بصمات أصابع يدها اليمنى باليسرى لكي تتسلل مجدداً لداخل اليابان. وتمت إعادة زرع رؤوس أصابع كل يد على اليد الأخرى. فنجحت الحيلة، وتم إدخال لين بنجاح. لكن السلطات لاحظت بعد بضع أسابيع الندبات الغريبة على رؤوس أصابعها، عندما كانت تحاول الزواج برجل ياباني يبلغ من العمر خمسةً وخمسين عاماً. وذكرت الشرطة اليابانية أن الأطباء الصينيين قد أقاموا تجارة مزدهرة من الجراحة البيومترية، وكانت لين هي الشخص التاسع الذي يتم اعتقاله ذلك العام بسبب التحايل عن طريق الخضوع لجراحة بيومترية.

من نافل القول إن مثل هذه الإجراءات القاسية ليست ضرورية حين يتمكن المخترقون من اعتراض بيانات البصمات أثناء إرسالها من جهاز الاستشعار البيومتري المزود بتقنية إنترنت الأشياء إلى مخدم الحاسب لمعالجتها، وهو ما وضحه مات لويس، الباحث في المجال الأمني، مسبقاً في مؤتمر بلاك هات للقراصنة في أوروبا. فقد ابتكر لويس أول مسجِّل حيوي في التاريخ، وهو المعادل لمسجل ضربات المفاتيح الخبيث. فبدلاً من تسجيل كل أزرار المفاتيح التي ينقر عليها أحدهم على جهاز الحاسب الخاص به، يمكنه أن يسرق صور بصمات الأصابع التي تقوم الماسحة الضوئية المصابة بمعالجتها. وقد استعرض لويس كيف يسمح له المُسجّل الحيوي بتحليل وإعادة استخدام البيانات التي التقطها، لتجاوز الأنظمة البيومترية بما يضمن له الدخول لأبنية يفترض بها أن تكون "أبنية آمنة". ربما كان من المغري الاعتقاد بأن أنظمة التعريف البيومترية منيعة بطبيعتها مقارنة بنظام كلمة المرور القديم، وهو افتراض لا يصح سوى حين يتم تحقيق هذه الأنظمة الجديدة بطريقة أكثر أمناً. وإلا فإن الأمر أشبه بتعبئة خمرٍ قديم في زجاجة جديدة.

كلمة مرورك؟ إنها مكتوبة على وجهك

في فيلم الخيال العلمي "ماينوريتي ريبورت" (تقرير الأقلية)، يؤدي "توم كروز" دور ضابط شرطة في العاصمة واشنطن في عام 2054. وفي أحد المشاهد، وبينما يتجول جون أندرتون، الشخصية التي يؤديها كروز، في أحد المراكز التجارية المحلية، يتم التعرف على وجهه من قبل اللوحات التفاعلية التي تقوم بتوجيه التحية للمحقق بالاسم، وتقدم له إعلانات بناء على تاريخ عمليات الشراء السابقة التي قام بها. يبدو أن عام 2054 قد جاء بشكلٍ أسرع من المتوقع. فمثلما يمكن لبصمات الأصابع أن تحدد هوية المرء بدقة، كذلك تستطيع بصمة الوجه والصور البيومترية لملامح وجهك،

مثل المسافة بين عينيك وأنفك وأذنيك وشفتيك. فهذه الخصائص البيومترية لن تكشف هويتك الشخصية فحسب، بل ستسمح أيضاً بتصنيفك من قبل الآخرين حسب الجنس والعمر والعرق والإثنية. كل هذه البيانات هي منية المسوقين المتعطشين لإعادة إنتاج تجربة الإعلان المستهدف التي تم تطبيقها على السيد أندرتون.

بالعودة إلى عالم اليوم، تطل لوحات الإعلانات في اليابان منذ الآن على المارة، فتقارن ملامح وجوههم بالزمن الحقيقي مع قاعدة بيانات إن.إي.سي، التي تحتوي على أكثر من عشرة آلاف نموذج تم تعريفه مسبقاً، ليتم فرز الأفراد بدقة وفق تصنيفات متنوعة للمستهلكين، ويتم تغيير الرسائل الإعلانية المعروضة وفقاً لنتائج التقييم الديمغرافية. وبعيداً من الإعلان، ثمة العديد من الاستخدامات الأخرى لتقنية التعرف على الوجه. إذ تسمح شركة فيس فيرست البيومترية في كاليفورنيا لبائعي التجزئة بمسح وجوه كل الزبائن في محالّهم للتعرف على السارقين. وفي حال تم التعرف على أحدهم، يرسل البرنامج على الفور بريداً إلكترونياً ورسائل نصيّة تحتوي على صورة للص المشتبه به، لكي يقوم الموظفون باتخاذ "الإجراء المناسب". وثمة نظام مشابه تعتمده فنادق هيلتون يستخدم تقنية التعرف على الوجه لمسح وجوه جميع الضيوف، ما يمكِّن الموظفين من إلقاء التحية على الضيوف بالاسم، وخصوصاً الأعضاء الذين يحملون بطاقة في.آي.بي الذهبية.

ليس المعلنون وحدهم من يمكنه الوصول لبيانات تعريف الوجه، بل ثمة مستهلكون آخرون يمكنهم ذلك أيضاً. فلقد لاحظ العديد منا وجود كاميرا عند مدخل بارٍ مجاور واعتقد ببراءة أن هذه الكاميرا موجودة في حال تعرض البار للسرقة. ولكن عندما تتصل كاميرا تقليدية بإنترنت الأشياء أو أدوات تحليل البيانات الضخمة، يصبح لدينا جهاز استشعار ذكي جديد. وقد تعاونت إحدى الشركات في مدينة أوستن بولاية تكساس مع النوادي

المحلية والملاهي الليلية لكي تأخذ كل تسجيلات الفيديو "بالجملة"، لتجري تحليلاً للوجه بالزمن الحقيقي لكل زبائن البارات. وكانت النتيجة هي تطبيق يسمى "سين تاب"، يمكّن هؤلاء الذين يريدون قضاء وقتٍ ممتع في أوستن من أن يحصلوا على إحصاءات مباشرة من كل مكان وأن يعرفوا أي النوادي الليلية ممتلئة ومختلطة إلى جانب أعمار الموجودين بالنادي. على سبيل المثال، يمكن أن تُظهر لوحة التحكم الخاصة بالتطبيق أن بار ومطعم ميْين ستريت ممتلئ بنسبة 47% بنسبة 68% من النساء بمعدل عمرٍ وسطي يبلغ 29، ونسبة 32% من الرجال بعمر وسطي يبلغ 26. يغنينا هذا التطبيق الفعال عن جهد التخمين والتنقل بين البارات، ويسمح لفتيان الأخويات الجامعية السكارى بتجنب "حفلات الذكور"، واختيار البارات التي تحتوي على أكبر عدد من النساء. فهل يمكن للتطبيقات المستقبلية أن تسمح للمستخدمين بالحصول على بيانات ديمغرافية أخرى لروّاد الحانة مثل الطول والوزن والانتماء الإثني؟ ربما يتحقق ذلك مع عدم وجود قوانين أو قرارات تحمي الأميركيين من التقنيات البيومترية المؤذية أو تتحكم بحدود استخداماتها.

لقد حسَّنت تقنيات التعرف على الوجه من معدلات المطابقة التي تحققها بشكلٍ لافت، وباتت دقتها الآن تصل إلى 98%، بنسبة تحسن قدرها 20% بين عامي 2004 و2014. فقد قامت جميع شركات الإنترنت الكبرى، ومن ضمنها آبل وغوغل باستثمارات لا يستهان بها في قطاع الأنظمة البيومترية للتعرف على الوجه، لكن لم يكن أيٌّ منها ضخماً مثل الاستثمار الذي قام به فايسبوك، حين اشترى شركة الأنظمة البيومترية الإسرائيلية الناشئة "فايس دوت كوم" عام 2012 بما يقارب 100 مليون دولار. يقوم موقع فايسبوك بالتعرف على الوجوه الموجودة في كل صورة تقوم بتحميلها (وهو ما وافقت عليه بنفسك ضمن اتفاقية شروط الخدمة

المؤلفة من تسعة آلاف وثلاثمئة كلمة). لقد تمكن فايسبوك بعد حصوله على "فيس دوت كوم" من تحسين خاصية "اقتراحات وسم الوجوه" لديه تحسيناً كبيراً والتعرف على كل الأشخاص في الصور التي تنشرها، باستخدام الخوارزميات البيومترية وعبر تشجيعك على وسم أصدقائك، وتأكيد صحة هوياتهم البيومترية لدى زوكربيرغ. لم تمر التقنيات الآلية للتعرف على الوجوه لدى فايسبوك بدون أن تثير الجدل نظراً لآثارها الواضحة على الخصوصية، وقد حظر صانعو القوانين في أنحاء الاتحاد الأوروبي هذه الخاصية. في هذه الأثناء، إذا عدنا إلى الولايات المتحدة، لا يوجد أي قانون يمنع تشغيل البرامج الخاصة بالتعرف على الوجه على مخزن الفايسبوك حيث منتجه، أي أنت كما ذكرنا سابقاً. لقد تم تحميل أكثر من ربع ترليون صورة منذ تأسيس فايسبوك، أي إن فايسبوك، وليس برنامج "أدهار" في الهند، هو أكبر مستودع للبيانات البيومترية على كوكب الأرض، تتخطى البيانات التي يحتويها أي مخزون تملكه أي حكومة في العالم.

يمكنك أن تتوقع المزيد من الضغط من "وول ستريت" لأجل تحويل البيانات البيومترية إلى نقود، وما من خشية من نقص في الزبائن، ومن ضمنهم الحكومة. فقد ادَّعى مسرِّب وكالة الأمن القومي إدوارد سنودن ضمن سلسلة تسريباته، أن وكالته قامت بالتنصت المباشر على مخدِّمات تسع من أكبر شركات الإنترنت، ومن ضمنها فايسبوك، ما قد يكون قد سمح للأوساط الاستخبارية بالوصول إلى منجم الذهب البيومتري الخاص بالشركة. وفي فضيحةٍ منفصلة، كشف سنودن أن الوكالة كانت بالفعل تجمع ملايين الصور الإضافية المنشورة على الإنترنت بشكلٍ يومي، وكانت قادرة على معالجة خمسة وخمسين ألف صورة يومياً على الأقل، معالجةً "لا تقل جودة عن التعرف على الوجه". فما الذي قد تفعله الشرطة والأجهزة الأمنية التابعة للحكومات بهذه البيانات البيومترية؟ في المجتمعات

الديمقراطية، يبقى الأمل بأن تُستخدم للقبض على المجرمين العنيفين والإرهابيين. ولكن بعد أن تُنصب مصيدة الاعتقالات البيومترية هذه، تصبح غايات استخدامها بيد أصحاب السلطة. ففي عالمٍ سري ليس فيه سوى القليل من الرقابة، لا بدَّ أن تحصل انتهاكات، وعندما تصبح هذه الأدوات بيد الطغاة والقادة الديكتاتوريين ستتحول إلى أساس الديستوبيا الأورويلية المماثلة لجهاز الأمن في ألمانيا الشرقية الشتازي.

كانت الشرطة في بريطانيا من أوائل من طبقوا التقنية السائدة للتعرف الآلي على الوجوه، باستخدام تقنية "نيو فايس" من شركة "إن.إي.سي"، لمطابقة الوجوه المأخوذة من أي صورة أو فيديو من مسرح جريمة مع قاعدة بيانات من الصور. وعندما تجتمع آلية التعرف على الوجوه مع أعلى كثافة لكاميرات الدائرة التلفزيونية في أي بلدٍ في العالم، تقوم بالتصوير بشكلٍ مستمر بينما يحملها رجال الشرطة، إضافة إلى تطبيقات الهاتف الذكي الأشبه بما نراه في مسلسل سي.إس.آي القادرة على إجراء التعرف على الوجوه وعلى بصمات الأصابع في مسرح الجريمة في آنٍ معاً، يبدو الأمر كما لو أن أيام الملاحقة الجنائية في فيلم ماينوريتي ريبورت قد جاءت بالفعل. فما مدى التقدم الذي أحرزته تقنيات التعرف على الوجوه حتى الآن؟ ما يكفي لمطابقة وجهك مع حسابك على الفايسبوك خلال ستين ثانية بينما تمشي في الشارع، ومع رقم ضمانك الاجتماعي بعد ستين ثانية أخرى. أما البرنامج الذي يجعل كل ذلك ممكناً فهو بيت.بات الذي بدأ كمشروع بحثي في جامعة "كارنيجي ميلون" بعيد أحداث الحادي عشر من أيلول تدفقت عليه ملايين الدولارات كتمويل من وكالة مشاريع أبحاث الدفاع المتطورة "داربا".

بينما تقوم المزيد من قوات الشرطة باستخدام الدوائر التلفزيونية لمراقبة مجموعات الأفراد التي تتجول في شوارع مركز المدينة أو في ستاد لكرة

القدم أو في أحد المطارات، يمكن لبرامج مثل بيت.بات أن تعمل في الخلفية بالزمن الحقيقي للتعرف على وجوه المارة، لتضع بعناية فوق رأس كل فرد فقاعة تشبه تلك التي نراها في أفلام الكرتون، تحتوي على رابط يؤدي للحصول على المزيد من المعلومات. وبنقرة بسيطة على الفقاعة يمكن مشاهدة حساب الشخص على الفايسبوك ورقم ضمانه الاجتماعي وتاريخه الائتماني وجميع الصور السابقة التي تم نشرها له على الإنترنت، سواء كانت صورة لرحلةٍ عائلية إلى ديزني لاند أم صورة له وهو يحمل كأس المارتيني في حفلة الشركة لعيد الميلاد، أو حسابه الخاص على موقع "ماتش دوت كوم". وبينما قد يدعم البعض حق قوات الشرطة في الوصول إلى تقنيات التعرف على الصور المتطورة هذه بهدف الحفاظ على السلامة العامة، فإن مشاعر هؤلاء ستختلف إذا أصبحت قدرات المراقبة القوية هذه بيد القطاع الخاص. لقد تأخرنا كثيراً.

قامت غوغل في منتصف عام 2011 بشراء بيت.بات، لتفتح الباب أمام محرك البحث العملاق لتحقيق التقنيات الضخمة للتعرف على الوجه في مجموعة منتجاته، ومن ضمنها يوتيوب وبيكاسا وغوغل بلس وأندرويد. وربما يكون المرشح الأوضح الذي يمكنه الاستفادة من تقنية التعرف على الوجه المدمجة هو نظارات غوغل. فباستخدام هذه الأداة، سيصبح من الممكن التعرف مباشرة على تلك الفتاة المثيرة أو الفتى المثير في الحفلة، ولن تقلق أبداً من نسيان اسم ذاك الموظف من قسم المحاسبة مجدداً. خوفاً من أي رد فعل شديد، تحظر غوغل استخدام تطبيقات نظارات غوغل للتعرف على الوجه في الوقت الحالي، ولكن مع شراء بيت.بات أصبحت المقدرة التقنية موجودة بشكلٍ كامل. أما القراصنة فقد حرّروا نظارات غوغل التي ابتاعوها بالطبع وقاموا بتطوير مجموعة من تطبيقات التعرف على الوجه، من بينها تطبيق نيم.تاغ الشائع.

يسمح نيم.تاغ للمستخدمين بمسح وجوه من أمامهم ومقارنتها مع ملايين السجلات المتوافرة على الإنترنت لاستعادة اسم الشخص وحساباته على الوسائط الاجتماعية، بما فيها حسابه على فايسبوك وتويتر وأنستغرام وغيرها من التفاصيل التي تشكّل هويته. ولا تقتصر تطبيقات التعرف على الوجه على نظارات غوغل، بل يمكن استخدامها بالسهولة نفسها مع الكاميرا الموجودة في هاتفك الذكي. وتماماً كما في فيلم ماينوريتي ريبورت، نعيش جميعنا الآن عصر التعرف على الوجوه. لذا، لن يكون أحد بعد الآن مجرَّد وجه ضمن الحشود. فقد بات وجهك اليوم عبارة عن كتاب مفتوح يمكن قراءته بلحظة من قبل أي شخصٍ آخر، بما في ذلك الحكومة.

يملك نظام المليار دولار "نيكست جينيرايشن آيدينتيفيكايشن"، أو إن.جي.آي، لتحديد الهوية لدى مكتب التحقيقات الفيدرالي نحو 52 مليون صورة وجه يمكن المقانة بها، من ضمنها 4.3 مليون صورة لأفراد ليس لديهم أي سجل إجرامي. ويحتوي النظام أيضاً على سجلات لمئة مليون بصمة إصبع فردية، إلى جانب الملايين من بصمات راحات اليد وعينات الحمض النووي وصور القزحية. ولا يقتصر عمل هذا النظام على مسح صور عمليات السطو لمطابقتها، بل يمكنه تعقب المشتبه بهم عبر تمييز وجوههم ضمن الجموع بواسطة الكاميرات الأمنية التقليدية، أو مقارنتها مع الصور التي يتم تحميلها ونشرها على الإنترنت. ولا توجد تقنية بيومترية خالية من العيوب بالطبع، كما أن مسألة المطابقات الخطأ، أي مطابقة أشخاص بملفات إجرامية عند حصول تطابق بيومتري مع عدم وجود هذا التطابق في الحقيقة، لها عواقب خطيرة على الناس البريئة، كما رأينا مسبقاً مع تزايد مراقبة الإرهاب ولوائح الأسماء الممنوعة من السفر.

على الرغم من أن تقنية التعرف على الوجوه قد تبدو وكأنها الدواء الشافي لكل داء، فإن لهذه التقنية مشاكلها. فكما يمكن اختراق أجهزة

استشعار بصمات الأصابع، يمكن أيضاً اختراق أنظمة التعرف على الوجه، التي يتزايد استخدامها في فتح هاتفك الذكي أو حاسبك أو للدخول إلى مكتبك. وكل ما يتطلبه اختراق بعض هذه الأنظمة مثل تلك الموجودة على الحواسب المحمولة من "لينوفو" أو تطبيقات كلمة السر على الهواتف الذكية مثل "فاست أكسس أني وير"، هو التقاط صورة للشخص الذي تود انتحال شخصيته. وقد نجحت التقنية نفسها مع أجهزة مسح القزحية، لتسمح للمخترقين بإجراء هندسة عكسية على المعلومات البيومترية المخزنة في قاعدة بيانات آمنة، واستخدامها للحصول على صورة للقزحية جيدة بما يكفي لخداع معظم ماسحات الأعين التجارية.

ثمة تحدٍّ آخر يواجه خوارزميات أنظمة التعرف على الوجه، وهو أن مستوى الدقة يصل لـ 98 - 99 بالمئة حتى في أفضل الأنظمة. فربما يبدو معدل الخطأ هذا صغيراً، لكن نسب الخطأ قد تتراكم. فتصوَّر أن نظام للتعرف على الوجه يرتبط بلائحة مراقبة الإرهاب التي تم اعتمادها في مطار أوهير الدولي في شيكاغو. فمع خمسين مليون راكب يعبرون يومياً، يعني وجود خطأ بنسبة 1% أن 500,000 راكب سنوياً (أكثر من 1,300 يومياً) قد يتم احتجازهم أو اعتقالهم ظلماً بسبب خطأ حاسوبي. ولا شك في أن المشكلة ستتفاقم بسبب الأخطاء البشرية التي تحدث عند إدخال المعلومات، كما رأينا مع لوائح الرقابة الأمنية الموجودة حالياً، ما يؤدي لمطابقة صحيحة تقوم بها الكاميرات مع اسم مكتوب بطريقة خطأ ضمن قاعدة بيانات المطلوبين.

قد تكون عواقب أخطاء تحديد الهوية البيومترية قاتلة. فقد بدأت وزارة الدفاع الأميركية بإنشاء قدراتٍ بيومترية قادرة على الاستهداف وتحديد الهوية في أسطول الطائرات بدون طيار الخاص بها. كما قامت شركة بروغيني للأنظمة، المتعاقدة مع وزارة الدفاع والتي تعمل جنباً إلى جنب

مع الجيش، بتطوير طائرةٍ بدون طيار محمَّلة بنظام "بعيد المدى آلي بيومتري لتحديد الموقع والتعقب والوسم"، يسمح للمركبات الجوية المسيّرة بالتعرف على أي هدف بشري باستخدام الأنظمة البيومترية قبل تفجير الذخائر على رأس الهدف. في مثل هذه الحالات، سيكون أي خطأ في تحديد الهوية البيومتري كارثياً. فمستقبل الحروب هو التسيير الذاتي، مع وجود طائرات بدون طيار تصطاد وتتعرف وتقتل وفقاً لحسابات معتمدة على برمجيات لا على قرارات يتخذها البشر.

نظراً للانتشار الواسع للكاميرات وبرمجيات التعرف على الوجه، علينا بلا شك أن نتوقع أن يتبنى المجرمون هذه الأدوات ويستخدموها لمصلحتهم. إذ يمكن للمتحرشين بالأطفال أن يستخدموا الأنظمة البيومترية للتعرف على ذاك الطفل الذي أعجبهم في ملعب الحديقة. أما الإرهابيون، مثل منفذي هجوم مومباي من منظمة لاشكار - إي - طيبة الجهادية، فإن وجود تطبيق التعرف على الوجوه على هواتفهم المحمولة كان سيسمح لهم بالتعرف على رئيس البنك كي. آر. رامامورثي دون الحاجة لأن يلعبوا لعبة التخمين مع مركز التحكم الإرهابي في الباكستان للتعرف على هويته.

حتى شركة الجريمة بدأت باستكشاف تقنيات التعرف على الوجه وفقاً لمفوض الشرطة الاتحادية الأسترالية. ففي حفل تخرج المئات من قوات الشرطة الجديدة عام 2011، لاحظ المسؤولون رجلاً بين حشد العائلات التي تشاهد أحبّاءها وهم يتسلمون شارات الشرطة. إذ كان الرجل يحمل كاميرا مع عدسة مقرِّبة وظهر وهو يلتقط صوراً وجهية لكل الخريجين. وبعد احتجازه والتحقيق معه، علم المسؤولون بأن المصور الهاوي المتحمس كان عضواً في عصابة منظمة خارجة على القانون من راكبي الدراجات. وكان يعمل لحساب شركة الجريمة على الأرجح لإنشاء قاعدة بيانات من الصور، للتعرف على الوجوه بحيث يتعرف أعضاء العصابة على أي شرطي يحاول

التخفي أثناء عمله في التحقيقات التي تتناول منظمتهم في المستقبل. سيكون للأدوات البيومترية أثر عميق، ليس فقط على عناصر الشرطة الذين يعملون في الخفاء، بل على برامج نقل الشهود أيضاً. فكل شخص لديه حياة سابقة يود إخفاءها لأسبابٍ شخصية أو مهنية قد يجد أن الاستمرار بات مستحيلاً. وليست صفاتك الجسدية هي وحدها التي ستفضحك، بل تصرفاتك الصغيرة أيضاً.

أحسِن التصرّف

> يتم تسيير الكثير من الأعمال اليوم بشكلٍ آلي؛ ماذا سيحدث لو مددنا هذا المفهوم إلى مجالات مهمة في المجتمع مثل تطبيق القانون؟ ماذا سيحدث لو بدأنا بالتحكم بسلوك المجرمين أو الناس بشكلٍ عام مع آلات تحركها البرمجيات؟ تبدو هذه الأسئلة وكأنها من الخيال العلمي ولكنها ليست كذلك.
>
> خوسيه باديلها، مخرج أفلام برازيلي

عندما يفكر الناس بالأنظمة البيومترية، فإنهم غالباً ما يركزون على قياسات المواصفات التشريحية مثل أصابعنا ووجوهنا وأيدينا وأعيننا. ولكن ثمة مجموعة أخرى من الأنظمة البيومترية تُعرف باسم الأنظمة البيومترية السلوكية أو أنظمة القياس الحيوي السلوكي، أو "بيهافيومتريكس"، تقيس الطرق التي نتصرف وفقها نحن وأجسادنا لتتوصل إلى سمات من شأنها أن تكشف عنا أكثر مما تكشف بصمات الأصابع. فإيقاع ضرباتنا على لوحة المفاتيح وصوتنا ومشتينا وموجات أدمغتنا وضربات قلوبنا، كلها يمكن تحويلها إلى مقادير حسابية بطرقٍ تعطينا بصماتٍ مميزة تحدد هويتنا بشكلٍ فردي. ومثلما يزداد استخدام علم المقاييس الحيوي التشريحية في المجال الأمني لتحديد الهوية والتحكم بالدخول، سيتنامى أيضاً حقل القياسات الحيوية السلوكية، بل إنه بدا يجد تطبيقاته بالفعل.

فقد بدأت الشركات ومراكز الاتصالات حول العالم باستخدام القياسات الحيوية الصوتية لكي تعطي الزبائن بصماتٍ صوتية تميزهم. فالتسجيل الصوتي الذي تسمعه عند الانتظار يقول لك أن "قد يتم تسجيل هذه المكالمة بهدف ضمان الجودة"، يعجز عن إخبارك بحقيقة أن أحد الطرق التي تقيس بها رضا الزبائن عند المكالمات الهاتفية هي النبرة والمضمون والمصطلحات التي تقولها خلال المكالمة. علاوة على ذلك، وسعياً لمكافحة الاحتيال، تقوم الشركات بإنشاء قاعدة بيانات صوتية مسجَّلة ضخمة للزبائن، تنتج بصمات صوتية مميزة يمكن استخدامها في المكالمات الهاتفية المستقبلية، للتأكد من أن الشخص الذي على الجهة الأخرى من الخط يحمل البصمة الصوتية البيومترية نفسها التي تم تخزينها. وحين لا يتطابق الصوتان، يتم توجيه أسئلة للتحقق بشكلٍ أدق من الشخص في عملية لا تمتاز بالحد الأدنى من الشفافية بالنسبة لعامة الناس.

تعمل "داربا" (وكالة مشاريع البحوث المتطورة الدفاعية) على تطوير تقنيات "المصادقة النشطة"، تركِّز على العملية الإدراكية لدى المستخدم وعاداته الشخصية والنماذج التي نتصرف جميعنا وفقاً لها، والتي من شأنها إذا ما جمعت مع بعضها أن تحدد هويتنا دون لبس. ويعرف أحد مجالات علم القياس الحيوي السلوكي باسم ديناميات ضربات المفاتيح، وهو يقيس الفروق الموجودة بين أساليبنا في الضرب على لوحة المفاتيح لكتابة أحرف معينة. وهي فروقٌ دقيقة تتعلق بترتيب الضرب على المفاتيح ومقدار قوة الضرب، بل إن طريقتنا في القص واللصق يمكن أن تعادل بصمات أصابعنا الإلكترونية أمام العالم. وتستخدم بعض الشركات مثل منصة كورسيرا للتعليم على الإنترنت أسلوب تحديد الهوية المعتمد على ضربات المفاتيح، لتتأكد من الطالب نفسه من يقوم بـ "حضور" كل درس افتراضي قبل أن تصدر شهادة التخرج.

تم تصميم منتج تايب.واتش من ووتشفول للبرمجيات، بحيث يعمل في الساحة الخلفية للشبكات ويراقب إيقاع نقرات المستخدم باستمرار، بغية كشف وإحباط محاولات الدخول غير المشروع. كما طوّرت شركاتٌ أخرى مثل شركة إيي.بي للقياسات الحيوية السلوكية في السويد، أدواتٍ تسجل كيف يمسك كل مستخدم هاتفه المحمول أو جهازه اللوحي، وحتى كيف يقوم كل شخص بتمرير أصابعه والضغط على الشاشة، لتكشف وقفاتٍ بين الأفعال المتنوعة لا يتجاوز طولها بضعة أجزاء من الثانية. وحدوث أي تغير في "البصمة الإدراكية" التي تم إنشاؤها سيطلق جرس الإنذار في المصرف ويمنع الدخول للحساب المصرفي، وهو أحد الأسباب التي دفعت أكبر مصارف الدانمارك، دانسكيه بنك، إلى تبني هذه التقنية. وتعتقد المصارف أن أدوات القياس الحيوي المشابهة من شأنها أن تخفض معدلات الاحتيال بمقدار 20%، لذا عليك أن تتوقع تعديل شروط الخدمة لدى المؤسسات المالية أو متاجر البيع بالتجزئة على الإنترنت التي تتعامل معها في المستقبل القريب، حيث ستطلب موافقتك على مثل هذه الرقابة التفصيلية قبل أن تسمح لك باستخدام تطبيقها المصرفي على الآيفون.

لا تنفك تظهر صيغ جديدة من القياسات الحيوية السلوكية. إذ تعتمد أساور المعصم نيمي مقياساً للفولت لقراءة ضربات قلبك، وتستخدم الإيقاع الفريد لكهربائية القلب لفتح حاسبك وهاتفك الذكي وسيارتك وبيتك. كما طوَّر علماء في مختبر الفيزياء الوطني في المملكة المتحدة نظام تحديد الهوية، عن طريق المشية يمكن استخدامه مع كاميرات المراقبة ليميِّز هوية الأفراد اعتماداً على مشيتهم. وثمة على أي حال طريقة أسهل للتعرف على هويتك اعتماداً على مشيتك، باستخدام مقياس التسارع في الهاتف النقال الذي تحمله على مدار الساعة ومشاركة هذه المعلومات مع شركة الهاتف النقال ومصنِّعي سماعات الهاتف ومطوّري تطبيقات الهاتف.

إذا كانت هذه التقنيات تبدو الآن تطفلية، فالواقع هو أنها قد تصبح أكثر تطفلاً بعد في المستقبل. فقد أقامت شركة موتورولا شراكة مع شركة إم.سي10 بهدف "تمديد قدرات الإنسان بوساطة وشوم إلكترونية غير مرئية يمكن ارتداؤها، تعمل بتقنية المعرّف الترددي الراديوي" ويمكن استخدامها للتحقق من كلمة السر. كما ابتكرت شركة "بروتيوس ديجيتال هيلث" قرصاً يمكنك ابتلاعه ويتغذى على أحماض معدتك، يمكنه أن يخلق لجسمك علامة مميزة بحجم 18 بايت لتتحول بأكملك إلى رمز متحرك لتعريف الهوية. وعلى الرغم من أن العديد من منتجات القياسات الحيوية الأمنية تقدم وعوداً جيدة، فإن القراصنة وشركة الجريمة لن يكفوا عن مساعيهم التي تحقق لهم إغناءً للذات ولن يعودوا أدراجهم مهزومين. لكن بدلاً من أن تخترق شركة الجريمة حاسبك، فإنها ستقوم باختراق الإنترنت التي في داخلك.

إذا ما وضعنا نقاط الضعف الأمنية جانباً، سنرى أن القياسات الحيوية والقياسات الحيوية السلوكية ستجلب معها مجموعة من القضايا المتعلقة بالسياسات العامة والخصوصية التي بدأت المجتمعات بالمعاناة منها للتو. فما تبعات القدرة على تحديد هوية أي شخص عن بعد وهو ينقر على لوحة المفاتيح في أي مكانٍ من العالم بالاعتماد فقط على طريقة ضربه للمفاتيح؟ إنه أمر عظيم من ناحية تحديد موقع المخترقين المطلوبين، ولكنه سيّئ بالنسبة لقائد الحركة المعارضة خلال الربيع العربي. إن التحدي الكامن في الرقابة البيومترية، سواء قام بها المعلنون في المركز التجاري المحلي أم جهاز أمن الدولة، هو أنها تؤثر على سلوكياتنا. فعندما نعرف أننا مُراقبون نتصرف بشكلٍ مختلف، وسنميل للانصياع وستصبح مراقبتنا أسهل. وسواء كانت بين يدي حكومات خارجة عن السيطرة أم شركات احتكارية كبرى، من شأن للتغيرات السلوكية الناتجة عن الرقابة الذاتية

التي أحدثتها الرقابة المنتشرة في كل مكان أن تقود الجميع سريعاً إلى مستقبلٍ بائس. ليست أجسادنا هي وحدها المعرَّضة لمثل هذه الرقابة المستمرة، بل ذواتنا الافتراضية أيضاً.

الواقع المعزّز

> بينما يتطور إنترنت الأشياء، سيقلّ وضوح الخط الفاصل بين الواقع والواقع الافتراضي، بطرقٍ مبتكرة أحياناً.
>
> جيف مولغان، بريطانيا، الصندوق الوطني للعلوم والتقنية والفنون

يبهرنا طوني ستارك في السينما بقدرات بدلة الرجل الحديدي الخارقة التي تستفيد، بالإضافة لميزاتها العديدة، بشكلٍ كبير من الضخ الهائل بالزمن الحقيقي لمعلومات الواقع المعزّز التي تمر أمام عينيه في الخوذة المزودة بشاشة عرض. وتعتمد التقنية في الفيلم بقوة على الحقيقة. إذ يتيح الواقع المعزز رؤية مباشرة وحية لبيئة العالم الحقيقي المادية عبر شاشة حاسوبية، كشاشة هاتفك النقال أو الشاشة المدمجة في نظارات غوغل، مع مراكبة معلومات رقمية إضافية مثل الصور أو الصوت أو الفيديو، أو بيانات الموقع الجغرافي على بيئة العالم الحقيقي. ومن أقدم تطبيقات الواقع المعزز تلك التي كانت تستخدم لوحات العرض بمستوى الرأس لطياري الطيارات المقاتلة، التي تتيح لهم رؤية معلومات النظام الحساسة على شاشات قمرة القيادة، دون أن يضطروا أثناء الاشتباك للنظر إلى الأسفل حيث المعدات. وقد باتت هذه التقنية موجودة في الحياة المدنية اليوم، حيث يقوم مصنعو السيارات مثل ميرسيدس بينز ورانج روفر بعرض سرعة السيارة والاتجاهات خطوةً بخطوة مباشرةً على الزجاج الأمامي للسيارة. وعلى عكس الواقع الافتراضي، الذي يستبدل الواقع الحقيقي بواحدٍ مصطنع، يحسِّن الواقع المعزز من إدراك الإنسان عبر وضع معلومات مفيدة فوق الأشياء التي نراها في العالم الحقيقي.

يمكن استخدام الواقع المعزز في أي شاشة تحتوي على أجهزة استشعار وكاميرات، سواء كانت شاشة هاتفك النقال أو حاسبك اللوحي أو نظاراتك الطبية أو حتى عدساتك اللاصقة. ومن المتوقع أن يصل عدد تطبيقات الواقع المعزز التي يتم تحميلها وتنصيبها سنوياً إلى 2.5 مليار بحلول عام 2017. ستكون فوائد الواقع المعزز مذهلة، والشركات الكبرى تستعرض لنا الإمكانات منذ الآن. ففي أحد إعلانات غوغل يسير أحد مستخدمي نظارات غوغل باتجاه مترو الأنفاق في مانهاتن، فيتلقى تحذيراً على شكل نافذة منبثقة، تظهر رسومياً في مجال الرؤية لديه على شاشة نظارته، عليها شعار القطار رقم 6 في هيئة النقل المدني تخبره بأن خدمة القطارات مغلقة. ستتيح أدوات كهذه للمسافرين حول العالم أن يرموا دليل السفر الضخم فودور وأن يستخدموا تطبيق الواقع المعزز ليأخذهم في جولة في المدينة.

بينما تمشي في الشارع، يمكن لهذه التطبيقات أن تراكب البيانات بحيث يمكنك أن ترى تقييم تطبيق "يلب" للمطاعم التي تمر بها ومعلومات "ويكيبيديا" عن التماثيل والأبنية التاريخية التي تقع في مجال رؤيتك. وسيمطرنا الواقع المعزز بوابل من الإعلانات بينما نتجول في المدينة بالطبع، حيث ستدرك نظارات غوغل الأجسام المادية المحيطة بنا وتضع الإعلانات فوقها. كما أدرجت شركة إيكيا الواقع المعزز في الدليل المصور لمنتجاتها عام 20، بحيث يتيح للمستخدمين التقاط صور للأرائك أو لأي قطعة أثاث أخرى بهواتفهم الذكية، ثم إدخال الصورة في منزلهم (بالأبعاد الصحيحة) ليروا كيف ستبدو قبل أن يقوموا بالشراء. سيصبح الواقع المعزز طريقتنا للتفاعل مع العالم المحيط بنا وبالأخص إنترنت الأشياء، ما يتيح لنا أن نسائل الأجسام المادية لنفهم أفضل تاريخها والغرض من استخدامها وسياقاتها. كما سيشكّل رابطاً بين العالم المتصل بالأنترنت والعالم غير المتصل بها ليغير كافة أوجه الحياة والعمل.

سيفرض الواقع المعزز مجموعة من الأسئلة المتعلقة بالأمن والخصوصية لا بد من مواجهتها. فقد يقوم أحد التطبيقات الخبيثة بمراكبة قيمة خطأ لحدود السرعة على إحدى لافتات الطرق العامة، أو وضع لافتة مزيفة في مكان لا يوجد أي شيء في الأصل، على شاشة عرض الواقع المعزز التي تم تركيبها على زجاج السيارة الأمامي. والأسوأ من ذلك أنه قد يظهر مجازاً مرورياً على طريق على أنه سالك، بينما يكون العكس هو الصحيح، ما قد يقود إلى حادث اصطدام بسيارة أخرى عند تبديل المجاز. وكما ذكرنا سابقاً، كلما انفصلنا عن الواقع وتقبلنا الواقع الافتراضي بدلاً منه، عرضنا أنفسنا للتلاعب وللهجمات التي تعتمد على "إيماننا بالشاشات".

إضافة إلى ما سبق، وكما قامت شركة الجريمة بتطوير برمجيات إجرامية مثل برنامج "بلاك شيدز" بهدف أتمتة الجريمة، علينا أن نتوقع منها أن تطلق عدداً من تطبيقات برمجيات الواقع المعزز الإجرامية في المستقبل. فعند استخدام هاتف الآيفون أو نظارات غوغل على سبيل المثال، يمكن للقراصنة أن يتحروا كل أجهزة إنترنت الأشياء في منزلك أو مكتبك بصرياً، ليشاهدوا المعلومات المعروضة على شاشاتها بحثاً عن الأجهزة التي تحتوي نقاط ضعفٍ معروفة أو حتى أن يشاهدوا كلمة مرور غير محمية، ما يجعل اختراق إنترنت الأشياء أسهل مما هو عليه اليوم. ستقوم التقنيات التي تغير الواقع، مثل الواقع المعزز، بفتح الباب على مصراعيه لبيئات افتراضية ثلاثية الأبعاد أضخم من سابقاتها، مثل أنظمة الواقع الافتراضي، والتي يمكن تخريبها وإساءة استخدامها بطرقٍ خطيرة.

صعود الإنسان الافتراضي

> الحقيقة هي مجرد وهم، حتى لو كانت وهماً شديد الحضور.
>
> ألبرت أينشتاين

بينما نعيش حياتنا من خلال شخصيات افتراضية، أو أَفَتارات، تمثلنا في

ألعاب الفيديو وعوالم الإنترنت ومواقع التواصل الاجتماعي، يزداد تمثيل هذه الذوات الشبكية لنا في المناسبات الاجتماعية والعمليات التجارية وحتى في الاتصال الجنسي. إنها تمثلنا على الإنترنت على مدار الساعة، تستغل الوقت والمساحة لتتفاعل بالنيابة عنا مع بقية العالم حتى أثناء نومنا. ذَكَرَ مصمم الألعاب المشهور جين ماك.جونيال أن "الإنسان اليافع العادي يراكم 10,000 ساعة من اللعب حتى سن العشرين"، تجسده في معظمها شخصية افتراضية أو إحدى شخصيات الألعاب. وبينما يقومون بذلك، نشهد نحن صعود الإنسان الافتراضي، الذي ربما يكون التطور الثاني للإنسان العاقل. إنه نوعٌ جديد بعيد من القيود الموجودة في العالم المادي الطبيعي يستفيد من الفورية والشعور بلامحدودية الإمكانات المتوفرة في العالم الافتراضي.

تستخدم الحقيقة الافتراضية الحواسب لخلق بيئات مصطنعة وعوالم حقيقية ومتخيلة، حيث يمكننا أن نُدخل وجوداً مادياً ليمثلنا نحن وحواسنا. فحتى حاسة اللمس يمكن إعادة خلقها بتطبيق تقنيات التغذية الراجعة اللمسية لـ "الشدة أو الاهتزاز أو الحركات" على المستخدم. ففي سياق تعليق مارك زوكربيرغ على عملية الشراء الأخيرة التي قامت بها شركة فايسبوك لأوكولوس ريفت، شاشة عرض الواقع الافتراضي العالية الاستجابة التي تثبّت على الرأس، والتي بلغت كلفتها 2 مليار دولار في بداية عام 2014، ذكر أنه "من الناحية الاستراتيجية نريد أن نبدأ ببناء ثاني أكبر منصة للحوسبة بعد الهاتف النقال". يمكن لأدوات مثل سماعات أوكولوس ريفت أن تنقلنا بلحظة لنعيش تجربة غامرة في فيلا جميلة في توسكانيا، أو في مقعدٍ في الصف الأول في إحدى مباريات الدوري الأميركي لمحترفي كرة السلة، أو معركة متخيلة ولكن واقعية بين شعبي الروملان والكلينغون.

تعد لعبة سيكوند لايف أحد أول العوالم الافتراضية، وتم إطلاقها من قبل

فيليب روزيديل من مختبر ليندن عام 2003، حيث كانت تتيح للمستخدمين أن يقدموا أنفسهم على شكل شخصيات افتراضية عالية التخصيص. وتتيح لك اللعبة أن تقيم الصداقات وتتسوق وتتعلم وحتى أن تحضر حفلاً لموسيقى الروك لفرقة يوتو تقوم بها الشخصيات الافتراضية الحقيقية لأعضاء الفرقة. وهناك شكلٌ آخر شائع من العوالم الافتراضية يعرف باسم "لعبة تقمص الأدوار الجماهيرية المتعددة اللاعبين على الإنترنت" أو "إم.إم.أو.آر.بي.جي". وهي عبارة عن ألعاب فيديو "تسمح لآلاف اللاعبين بالدخول بشكلٍ متزامن إلى العالم الافتراضي والتفاعل بعضهم مع بعض، حيث يمكن للاعبين أن يديروا مدنهم وبلدانهم وجيوشهم الخاصة"، للدخول في المعارك والقيام "بمجموعة متنوعة من المهام من خلال شخصياتهم الافتراضية". وتعد لعبة وورلد أوف واركرافت من شركة بليزارد إنترتينمنت إحدى أكبر ألعاب تقمص الأدوار المتعددة اللاعبين على الإنترنت، حيث جذبت أكثر من اثني عشر مليون متابعٍ، يقوم كل منهم بدفع الأجور الشهرية ليسكن في عالمٍ افتراضي. ولكن على الرغم من درجة التعقيد وتعدد الطبقات التي تقوم عليها هذه المساحات الافتراضية اليوم، يشير روزيديل إلى مستقبلٍ قريب تتطور فيه البرمجيات والمعدات، مثل المنصات العالية الدقة، لتقدم لنا الجيل الثاني من العالم الافتراضي على شكل عالمٍ قد يكون من التعقيد والضخامة بما يضاهي العالم الحقيقي اليوم.

لكي يستطيع المرء فهم العوالم الافتراضية، عليه أن يفهم أولاً عقلية ونفسية الأشخاص الذين يسكنون المساحات الافتراضية. إذ ينظر الكثيرون بجدّية لـ "حياتهم الثانية" على أنها "حياتهم الأولى"، كما أن 20% من لاعبي إم.إم.أو.آر.بي.جي ينظرون إلى عالم اللعبة على أنه مكان إقامتهم "الحقيقي". فبالنسبة لهم، الأرض هي مجرد مساحة مادية، أو منزل ثانوي يمكن فيه للّحم الذي تتكون منه أجسادهم المادية أن يأكل وينام، بينما

تتم معظم علاقاتهم الشخصية والتجارية والجنسية على الإنترنت. وبينما لا تشعر الأكثرية الساحقة من مستخدمي الحقيقة الافتراضية بالمشاعر نفسها، قد تصبح هذه المشاعر مألوفة عندما نمضي وقتاً أكثر في بيئات افتراضية غامرة وممتعة.

ولكن ثمة مساوئ لهذه المتعة الافتراضية كما تبين لزوجين في كوريا الجنوبية أمضيا الكثير من الوقت في أحد مقاهي الإنترنت المحلية، لرعاية ابنتهما الافتراضية في عالم الإنترنت المعروف باسم بريوس على نحو هوسي، هاجرين المنزل لأيام دون إطعام طفلتهما الحقيقية البالغة من العمر ثلاثة أشهر، ما أدى لموت الرضيعة في العالم الحقيقي. قد تبدو هذه الحالة متطرفة، لكن تم تسجيل العديد من هذه الحالات مع مرور السنوات، وهي قد تتكرر في المستقبل.

إن الخط الفاصل بين الإنسان والآلة، وبين الاتصال بالإنترنت وعدم الاتصال بها، يبدو مبهماً أكثر فأكثر. وسيعرف كل من لعب يوماً بلعبة فيديو فوق واقعية، من نمط اللاعب الواحد الذي يطلق النار مثل "دوم" أو "كال أوف دوتي"، أن هذه التجربة الافتراضية ستؤدي حتماً لتغيرات فيزيولوجية، من ضمنها تسارع ضربات القلب والتعرق براحة اليد عند احتداد المعركة. ولأن الشخصيات الافتراضية هي ممثلة لنا ولأن الناس يمضون آلاف الساعات متقمصين شخصياتهم الافتراضية، يزداد تداخل أرواح العالم الحقيقي مع تمثيلات العالم الافتراضي. والحقيقة هي أن ما يحدث لشخصيتنا الافتراضية يترك أثره علينا. وكل جريمة تحدث عادةً في العالم الحقيقي تقريباً يمكن إعادة نسخها لتأخذ مكانها في العوالم الافتراضية. فلدى العوالم الافتراضية عملاتها الخاصة، مثلا دولارات ليندن أو الذهب في وورلد أوف واركرافت، والتي يمكن تحويلها إلى مالٍ حقيقي كما هو الأمر مع العملة الرقمية "بيتكوين". كما أنها أصبحت الهدف المفضل لشركة

الجريمة التي تطلق 3.4 مليون هجمة يومياً سعياً وراء حسابات اللاعبين على الإنترنت.

بقدر ما يبدو الأمر غريباً، يزداد انتشار الجرائم المرتكبة من قبل الشخصيات الافتراضية أو ضدها، فمن الممكن أن تتعرض أنت في العوالم الافتراضية لكل شيء بدءاً بالتهديد الافتراضي وصولاً إلى انتحال الشخصية. وقد اعتقلت الشركة اليابانية رجلاً بسبب سلسلة من عمليات سلب الشخصيات الافتراضية. حتى إنه تم تسجيل "اعتداءات جنسية" في العوالم الافتراضية، كما في عام 2007 في حادثة تم التحقيق بها من قبل الشرطة البلجيكية الفيدرالية. وفي الحادثة أصيبت الشخصية الافتراضية الخاص بامرأة ببرنامج خبيث انتقل إليها عبر رجلٍ قابلته في لعبة سيكوند لايف. وأتاح الفيروس الحاسوبي للمعتدي أن يتحكم بالشخصية الافتراضية الأنثى ويعتدي عليها جنسياً بطريقة عنيفة ودموية. وفي نهاية الأمر، تم التحقيق بالحادثة على أنها حادثة "دخول غير مشروع لنظام حاسب". وبينما قد يجد البعض أنه من السهل أن يتم رفض قضية كهذه جملة وتفصيلاً، فإن ذلك سيكون أكثر صعوبة في المستقبل نظراً للمساحة الافتراضية التي تزداد اتساعاً باستمرار والصدمة الحقيقية المحتملة التي يمكن أن تسببها مثل تلك الحوادث مع مضي الزمن. يمكن لهذه الحوادث أن تتفاقم مع العدد المتزايد لأجهزة رد الفعل اللمسي المادي، والتي يتم وصلها بشكل متزايد مع عوالم الإنترنت، ما يتيح للعشاق أن يستخدموا الـ "تيليديلدو"، أو "أدوات ممارسة الجنس عن بعد"، ليثيروا بعضهم عن بعد عبر الإنترنت. وكأي غرض مزود بإنترنت الأشياء، ستكون هذه الأدوات عرضة للاختراق، ما قد يفتح الباب على عواقب غير مسبوقة.

قد يؤدي صعود الواقع الافتراضي لما هو أكثر من العواقب الجنائية ويصل بالأمر إلى مسائل الإرهاب والأمن القومي. وقد ذكر تقرير لرئيس

الاستخبارات القومية في الولايات المتحدة عام 2008، أن الإرهابيين قد يستخدمون المساحات الافتراضية لإجراء اتصالاتهم الخفية، ولنشر الدعاية وتدريب العناصر ولغسيل الأموال الافتراضية، بل حتى تجنيد أتباع جدد. ووفقاً لملفٍ من اثنتين وثمانين صفحة قام إدوارد سنودن بتسريبه ونشره على موقع "نيويورك تايمز" الإلكتروني، فإن وكالة الأمن القومي ومكاتب الاتصالات الحكومية البريطانية كانت تقوم بالتجسس على اللاعبين في العوالم الافتراضية، بمن فيهم لاعبو وورلد أوف واركرافت وسيكوند لايف، إلى جانب مجموعة متنوعة من الألعاب التي تقدمها منصة إكسبوكس من مايكروسوفت. وقد قام الجواسيس بإنشاء شخصيات افتراضية متخفية "لكي تتجسس وتحاول تجنيد مخبرين، بينما تقوم هي نفسها بجمع المعلومات"، وللقيام باعتراضٍ شامل للاتصالات بين اللاعبين، بمن فيهم ثمانية وأربعون مليون شخص يستخدمون شبكة منصة إكسبوكس لايف.

مع استمرار النمو الكبير للواقع الافتراضي تضعف الفروق بين ذاتنا الافتراضية والواقعية أيضاً، وسندخل عالماً تزداد فيه صعوبة تحديد متى تنتهي ذاتك الحقيقية ومتى تبدأ ذاتك الافتراضية. إنها الإنترنت التي صرت جزءاً منها، وهي قابلة تماماً للاختراق. رأينا خلال هذا الفصل أمثلة عديدة عن كيفية تحول التقانة التي من حولنا إلى تقانة موجودة علينا وبداخلنا. فالأجهزة القابلة للارتداء والدمج والبلع والزرع بشكلٍ أو بآخر تجعلنا ننضم لأمة السايبورغ، ما يفتح أجسامنا المادية أمام الهجمات الافتراضية للمرة الأولى. وما يزيد من شدة هذه التحديات هو حقيقة أن تشريحنا وفيزيولوجيتنا يمكن قياسهما عن بعد، بعلمنا أو بدونه، باستخدام القياسات الحيوية والقياسات الحيوية السلوكية التي يمكنها تصنيفنا والتعرف علينا بشكلٍ لا لبس فيه. نتيجة لهذا، بات الفتات الرقمي يتسرب إلى العالم المادي، بينما نندمج نحن، بأجسادنا وذواتنا، في الفضاء السايبري

كما لم يسبق لنا من قبل. لكن كما سنرى، سيكون العكس صحيحاً أيضاً. فستترك الحواسب وغيرها من الأغراض التقنية الثابتة العالم الافتراضي وراءها قريباً لتنضم لنا وتتحرك في الفضاء الحقيقي. بعد فترة طويلة من السبات، بدأت الآلات بالحياة أخيراً، وها هي جاهزة لتهبط إلى عالمنا المادي. وعندما ستقوم بذلك، ستجلب معها موجة مدٍّ عاتية من التهديدات التي لم نتحضر لها أبداً.

الفصل الخامس عشر
فجر الآلة عندما تصبح الجريمة السايبرية ثلاثية الأبعاد

لن تدرك مدى تسلط الآلات إلا حين ترتكب خطأً.

كليف جيمس

نشأ رضوان فردوس في أشلاند في ماساتشوستس، وهي بلدة مترفة في ضواحي بوسطن. وكان والداه قد هاجرا من بنغلادش سعياً وراء عيش أفضل في أميركا، عاقدين آمالاً كبيرة على ولدهما الذي أنشآه على تقوى الله والإيمان بالإسلام. وبعد تخرجه في الثانوية، حصل فردوس على درجة الإجازة في الفيزياء من جامعة نورثويسترن عام 2008. لكنه بعد أن عجز عن إيجاد عمل معقول في مجاله، عاد ليسكن مع والديه. وكان على غرار كثيرين من بني جيله يمضي الكثير من الوقت على الإنترنت. ثم راح يتردد على مواقع إسلامية متطرفة تحرض على الجهاد ضد الشيطان الأعظم، أي أميركا.

ومع مرور الوقت، ازداد يأس فردوس في الولايات المتحدة وقرر أنّ وقت الفعل قد حان. ثمّ أسرّ لرجل في المسجد المحلي بأنه يرغب في الانضمام إلى القاعدة، وتم تقديمه إلى العديد من "الإخوة" الذين يمكنهم مساعدته في مسعاه. وفي عام 2010، بدأ فردوس بالتخطيط لهجوم عنيف يقوم به بنفسه مستهدفاً الكفار الذين كان يرى أنهم يحيطون به من كل صوب في أميركا. وكانت خطته، وإن لم تكن على قدر كبير من الابتكار بالنسبة لإرهابي، تقوم على استخدام روبوتات قاتلة، حيث قام فردوس بشراء ثلاث طائرات مسيّرة كان ينوي تحميلها بمتفجرات السي - فور وتوجيهها جواً صوب الكونغرس الأميركي والبنتاغون.

وكانت تلك الطائرات المسيّرة طائرات يتم التحكم بها عن بعد، بُنيت كنماذج مستنسخة بدقة بقياس العُشر لطائرات الشبح إف - 4 التي تستخدمها البحرية الأميركية، وتتوفر على الإنترنت عبر مواقع هواة

الطائرات المسيّرة. وكانت هذه الطائرات قادرة على حمل ما يصل إلى أربعين باونداً والطيران بسرعة 160 ميلاً في الساعة بفضل المحركات النفاثة المزودة بها. ويمكن توجيهها عن بعد بواسطة مشغّل على الأرض باستخدام جهاز بث راديوي يُحمل باليد، كما يمكنها أيضاً، وكانت هذه خطة فردوس، أن تطير مستقلة على طول مسار جوي يعطى لها بفضل حساسات الموقع الجغرافي (جي.بي.إس)، ما يسمح بتحطيم الطائرة المسيّرة على الهدف المختار لها. وكان للطائرة مزايا أخرى أيضاً، فقد كانت الطائرات المسيّرة قادرة على الإقلاع والهبوط في أي مكان تقريباً، كما أن هذه الطائرات الصغيرة التي تطير على ارتفاعات منخفضة، يكاد يستحيل اكتشافها بواسطة الرادار. حين أبلغ فردوس أصحابه في القاعدة بخطته، تحمسوا لما أزمع عليه ووعدوه بالدعم والتمويل.

وباستخدام اسم مُنتحل وقصة ملفقة، طلب فردوس ثلاث طائرات من النموذج المذكور من مصادر مختلفة بكلفة 3000 دولار للواحدة. وسدد هذه المبالغ عبر حسابه على البايبال الذي أنشأه تحت اسم مستعار أيضاً، وطلب إيصال الطائرات إلى مخزن بالقرب من فرامينغهام كان قد استأجره وسدد أجرته نقداً. ثم بدأ فردوس بتجميع الأجهزة سراً قبل أن ينتقل إلى المرحلة التالية من خطته، وهي الحصول على المتفجرات. وفي ما يتعلق بهذا الهدف، أثبت أصدقاؤه الجدد في القاعدة أنهم قادرون على المساعدة إلى حد بعيد. فقد وفروا له 25 باونداً من متفجرات سي - فور، والعديد من الرمانات اليدوية وستة رشاشات كلاشنيكوف آلية، بينما بقي هو مختبئاً في مخزنه المغلق الذي كان بمساحة مئة متر.

ثم ارتحل فردوس إلى واشنطن العاصمة لكي يعاين أهدافه بدقة، فراح يلتقط الصور ويرسم نقاط الهجوم على خريطة. وقرر أن يكون مكان إطلاق الطائرات المسيرة هو حديقة إيست بوتوماك الموجودة في موقع

مناسب على المسافة نفسها من كلا الهدفين. وكان البنتاغون هو أول ما كان سيضرب مستهدَفاً بطائرتين تأتيانه من جهتي البناء المتقابلتين، موجّهتين كلتيهما صوب الطابق الرابع. ولم يكن على فردوس أن يكون على متن إحدى هذه الرحلات بالطبع. فقد قام ببناء محرك روبوتي مساعد لطائراته المسيّرة الذاتية التوجيه، قادر على سحب مسامير الرمانات اليدوية الست عشرة التي كان يزمع تثبيتها على متن كل طائرة يتحكم بها عن بعد. وكان المساعد الروبوتي على متن الطائرة سيُبَرمج بحيث يتفعّل قبل حدوث الارتطام بقليل ليسحب جميع مسامير الأمان لإحداث أكبر أثر ممكن.

وكانت خطة فردوس تشتمل، إضافة إلى الهجوم بالطائرات المسيّرة، على هجوم أرضي يقوم به فريقان من ثلاثة أشخاص يحملون رشاشات كلاشنيكوف لإطلاق النار على الأبرياء الذين سيهرعون هرباً من مكان الانفجارات التي ستدك بناءهم. وكانت المرحلة التالية في الخطة تقوم على استخدام طائرة مسيرة أخرى ذات توجيه عالي الدقة يتم التحكم بها عن بعد تحلّق باتجاه قبة الكونغرس فتدمرها وتجعلها شظايا.

عاد فردوس إلى بوسطن ووصّف خطة مهمته بتفصيل مدهش، اشتمل على مواصفات الطائرات المسيّرة والبروتوكولات البرمجية والخرائط والصور والمخططات وحدود الحمولات والمتطلبات المالية. وقدم الملف على وحدة تخزين يو.إس.بي إلى مخاطبيه من القاعدة، الذين عبروا عن إعجابهم الشديد بعرضه. ثم سألوه كيف تعلم كل هذا القدر عن الروبوتات والطائرات المسيّرة، فكان جوابه "تقانة الطائرات المسيرة في غاية البساطة. لا شك في أنك بحاجة إلى بعض الكفاءة، لكنني أقوم بأشياء من هذا القبيل منذ كنت طفلاً". واتفق الجميع على المضي في الخطة، وعاد فردوس إلى فرامنغهام لتفقد مخزونه من الأسلحة والمتفجرات. وما إن فتح باب المستودع حتى داهمته فرقة من العملاء الخاصين من مكتب التحقيقات

الفدرالي، ليكون ذلك أول هجوم إرهابي باستخدام الطائرات المسيّرة يتم إحباطه على الأراضي الأميركية.

وتبيّن لاحقاً أن المسلم الذي تقرب منه فردوس في مسجده المحلي لكي يقدمه إلى القاعدة كان مواطناً شريفاً اتصل بالشرطة فور سماعه لطلب فردوس. أما "الإخوة" الذين التقى بهم فردوس فما كانوا سوى عملاء متخفين لمكتب التحقيقات الفدرالي. وفي شهر تموز من عام 2012 أدين فردوس بتهمة محاولة تدمير مبنى فدرالي بالمتفجرات والدعم المادي لمنظمة إرهابية أجنبية، وحكم عليه بالسجن لمدة سبعة عشر عاماً. كما سبق ورأينا كيف يستخدم الجيش الطائرات المسيّرة بفعالية كبيرة في أنحاء العالم، فإن المجرمين والإرهابيين لا يقلون عنه قدرة على بناء هذه الأجهزة واستخدامها. وحين يتم إطلاق عدة طائرات مسيّرة من حديقة إيست بوتوماك وتسييرها بسرعة 160 ميلاً في الساعة محجوبةً عن الرادار، ستصيب هذه الطائرات هدفها في غضون دقائق دون أن تترك وقتاً لأحد للإخلاء أو الرد. ومع شيوع استخدام الطائرات المسيّرة وغيرها من التقانات الروبوتية، علينا أن نتوقع استغلالها من قبل جميع عناصر المجتمع، سواءٌ للخير أم للشر. وإذا كانت هجمات الحادي عشر من أيلول قد تمت عبر سيطرة بشر على طائرات ليحلقوا بها صوب أبنية مسكونة، فإن الإصدار الثاني من هذه الهجمات سيستغني عن دور البشر وسيستخدم الروبوتات عوضاً عنهم.

نحن، الروبوتات

> سيكون هناك في المستقبل، وأنا على يقين من ذلك، روبوتات أكثر بكثير في جميع مجالات الحياة. فلو قلت لأحد عام 1985 إن الحواسب ستتوفر في المطبخ خلال 25 عاماً، لما كان لذلك أي معنى بالنسبة له.
>
> رودني بروكس

عبر تاريخ السينما والتلفزيون، كنا نشاهد الروبوتات في مختلف الأدوار. فكان بعضها ودوداً وخدوماً مثل وول - إي وجوني رقم 5 في "دارة مقصورة"، وسي.3.بي.إو وآر2 - دي2 في حرب النجوم. بينما كانت روبوتات أخرى خطيرة هدفها تدمير البشرية، مثل غورت في "اليوم الذي توقفت فيه الأرض" وتي - 800.إس في الفاني. وبفضل التقدم المحكوم بقانون مور، لا تنفك الروبوتات تغادر الشاشة الفضية وتنضم إلينا في حياتنا. والتقدم الأسي لشرائح السيليكون والحساسات الرقمية والحوسبة الرقمية واتصالات الحزمة العريضة، كفيل بأن تصبح الروبوتات، تماماً كالحواسب والهواتف النقالة من قبلها، كلية الوجود في حياتنا.

تتزود الروبوتات على نحو متزايد بميزات متقدمة مثل الكاميرات لعالية الدقة وحساسات اللمس وأجهزة البحث الليزري، تجمع بينها كلها أدمغة حاسوبية. وتتحرك الروبوتات بفضل مشغّلاتها الميكانيكية، وهي عبارة عن محركات إلكترونية متصلة بتروس تدعم وتوجه عجلاتها وأرجلها وأذرعها، تماماً كما تحرك العضلات الكائنات البشرية. وقد تحققت تقدمات هائلة في مجال الروبوتيات مدفوعة في جزء لا يستهان به منها بثورة الهواتف الذكية، فالروبوتات تعتمد على الكثير من الشرائح الحاسوبية والبطاريات والحساسات التي يعتمد عليها الهاتف الذكي المتزايد القدرات الذي في جيبك.

بقي استخدام الروبوتات حتى اليوم محصوراً إلى حد كبير في مجال التصنيع، حيث تتولى مهام متكررة "خطرة ووسخة ورتيبة"، كتلك التي تعمل على خطوط تجميع السيارات. لكن الروبوتات تزداد تعقيداً اليوم، ومهاراتها وحواسها وذكاؤها في تطور، ما يسمح لها بتولي مهام أكثر تعقيداً بكثير. فقد باتت قادرة على السير والكلام والرقص وقراءة تعابير وجوهنا والاستجابة لأوامرنا الشفهية. وثمة روبوتات تعتني بالمسنّين وتعطل القنابل

وتقود السيارات وتعمل في محطة الفضاء الدولية وتقتل الإرهابيين في أنحاء العالم. وفي السنوات القادمة، سيزداد انخراطها في مجال إطفاء الحرائق وإيصال الطرود ومكافحة الجريمة وإجراء العمليات الجراحية والمساعدة في التعامل مع الكوارث وتأمين المرافقة. كما يزداد عدد الشركات الناشئة التي تعمل في مجال الروبوتيات إلى حد الانفجار، حتى إن البعض يقدّر أن تصل سوق الروبوتات الصناعية عام 2018 إلى 37 مليار دولار.

الروبوتات هي حواسب، أو أنظمة مؤتمتة قادرة على تجاوز السطح الثنائي الأبعاد الذي كان أسلافها محصورين فيه، بحيث تلمس العالم المجسم المحيط بها وتؤثر فيه وتتفاعل معه. ويمكن التحكم بمعظمها عن بعد عبر الإنترنت أو بواسطة تطبيقات الهاتف الذكي، الأمر الذي يسمح لجحافل من الروبوتات بالانضمام إلى إنترنت الأشياء. وثمة تبعات هائلة لذلك، فنحن نعيش، كما يلاحظ جوي إيتو، مدير مختبر الوسائط في معهد ماساتشوستس للتقانة، في حقبة تقارب، أي في زمن "تنصهر فيها بتّات العالم الرقمي مع الذرات هنا في العالم المادي".

تدخل الروبوتات فضاءنا الثلاثي الأبعاد وتشاركنا إياه. وكما جميع الأغراض المتصلة بإنترنت الأشياء، فإن الروبوتات بدورها عرضة للاختراق، ولو أن الآثار في حالتها قد تكون أعمق بكثير. فعبر تاريخها القصير، كانت الجريمة السايبرية تختبئ دائماً وراء شاشات الحواسب، أي إنها مشكلة ثنائية الأبعاد قد تؤثر على محفظتك أو على حسابك المصرفي ليس إلا. لكن هذه الجريمة السايبرية، بفضل التقدمات المتحققة في مجال الروبوتيات، ستخرج أخيراً من قيودها الافتراضية لتنفجر داخل فضائنا المادي. ونحن أبعد ما نكون عن الجاهزية لما هو قادم.

المجمّع العسكري - الصناعي (الروبوتي)

طوال عقود، كانت الروبوتات الصناعية تكدح جنباً إلى جنب مع الإنسان

العامل في المستودعات والمعامل، لكن الروبوتات الصناعية الحديثة باتت أيقونات هندسية قادرة على حمل المئات من الباوندات ونقل مختلف الأشياء مراراً وتكراراً بمعدل خطأ يبلغ أجزاء من الألف من البوصة، وهي مفخرة لا قدرة للبشر على مضاهاتها. وكانت هذه الآلات في البداية باهظة تصل كلفة الواحدة منها إلى مئات الآلاف من الدولارات وتحتاج إلى أشهر من البرمجة الحاسوبية المخصصة قبل أن تبدأ بإنجاز المهام المنوطة بها. وعلى الرغم من التكاليف، ما من صناعة استفادت من الروبوتات مثل صناعة السيارات التي كانت مسؤولة عن 40 بالمئة من مبيعات الروبوتات على مستوى العالم عام 2013. فالروبوتات تسرّع عملية إنتاج السيارات وتجعلها أكثر أماناً وأقل تكلفة وأكثر فعالية، وهي تنجز مهام الإنتاج المؤتمت لدى جميع المنتجين الكبار للسيارات، من فورد إلى بي.إم.دبليو. ففي معمل واحد لهيونداي في ألاباما، يعمل 500 روبوت بلا كلل على لحام قطع السيارات ودهانها وشدها ونقلها لإنتاج أكثر من ألف سيارة في اليوم. كما أعلنت أمازون عام 2014، كأنها لا تريد لأحد أن يتجاوزها، أنها تستخدم عشرة آلاف روبوت من إنتاج كيفا للنظم تتنقل في مخازنها الشاسعة لتحضر سلعاً محددة إلى الموظفين البشر الذين يغلفونها قبل تسليمها إلى روبوتات أخرى من أجل الشحن. وتقوم هذه الروبوتات بثلاث ورديات في اليوم لـ 365 يوماً في السنة دون أن تأخذ استراحة لاحتساء القهوة.

تنخفض تكلفة الروبوتات الصناعية وتزداد فعاليتها وسهولة تسخيرها بمعدل أسي، وربما ما من روبوت يوضح هذا التغير مثل باكستر، الرُوَيبِت الرخيص الظريف من إنتاج ريثينك روبوتيكس. فتكلفته البالغة 22 ألف دولار لا تتجاوز عشر تكلفة سابقيه. والأكثر إدهاشاً من ذلك هو أنه يعمل مباشرة بعد تشغيله، فلا يحتاج إلى أكثر من ساعة حتى يصبح في حالة

عمل، مقارنة بثمانية عشر شهراً كانت ضرورية لإدماج الجيل السابق من الروبوتات الصناعية في عمليات المصنع. ويستطيع باكستر تعلم القيام بعمليات بسيطة، مثل "التقاط وإلقاء" الأشياء على خط التجميع خلال خمس دقائق فقط. وهو يمتاز بوجه محبب يرتسم على الشاشة المركبة على رأسه وبذراعين ماهرتين تستطيعان الحركة بأي اتجاه وفق مقتضيات المهمة التي يتولى القيام بها. ولا يحتاج باكستر إلى برمجة خاصة، بل يستطيع التعلم بواسطة الرؤية الحاسوبية من خلال مراقبة عامل ينجز المهمة أمامه ليصبح الرويبت قادراً على تكرارها إلى الأبد. ومع انخفاض التكاليف أكثر بعد، ستصبح أسعار هذه الروبوتات منافسة حتى للعمالة القادمة من وراء البحار، بل إن الكثيرين يأملون أن تقود الروبوتات المحلية إلى نهضة جديدة في التصنيع الأميركي.

تظهر الروبوتات اليوم في كل مكان، من المطاعم إلى المستشفيات. ففي أكثر من مئة وخمسين مركزاً طبياً، يمكن استدعاء روبوتات تي.يو.جي من إيثون بواسطة تطبيق على الهاتف الذكي، لتتنقل آلياً عبر الممرات وتوزع أدوية المرضى ووجباتهم وبياضاتهم، وكلها أعمال كان يقوم بها الممرضون في السابق. وتسمح رويبتات طبية أخرى، مثل روبوت دافنشي الجراحي العفوي، للجراحين بالعمل على مرضاهم باستخدام أذرع روبوتية. فباستخدام شاشة موصولة بعدسة داخلية ومقبض تحكم، يمكن للأطباء مشاهدة داخل المريض بأبعاد ثلاثية وتوجيه أدوات جراحية صغيرة لتنفيذ إجراءات جراحية تتراوح بين استئصال الرحم وإصلاح صمام القلب. فمع الاستغناء عن إدخال أيدي البشر الضخمة إلى أحشاء المريض، يمكن تنفيذ العمليات الجراحية الروبوتية بأقل قدر من التدخل الخارجي، ما يخفّض مضاعفات العمل الجراحي بنسبة 80 بالمئة ويقصّر مدة التعافي إلى حد كبير. ويتم إجراء أكثر من 500,000 عملية من هذا القبيل في أنحاء العالم

كل عام. وباستخدام تقانة مشابة، يمكن للجراح أن يجري عملية لمريض عن بعد عبر الإنترنت بواسطة الجراحة البعيدة التي أجريت أول عملية منها عام 2001، حين قام جراح في نيويورك بإجراء عملية استئصال مرارة عبر الأطلسي لامرأة في ستراسبورغ بفرنسا.

على الرغم من المكاسب المدهشة التي أمكن تحقيقها في مجال الروبوتية الطبية والصناعية، فإن النمو الذي حققته الروبوتية العسكرية بات مذهلاً. ففي عام 2003، كان لدى البنتاغون أقل من خمسين طائرة مسيّرة في ترسانته. أما اليوم، فباتت الولايات المتحدة تتجاوز جميع البلدان الأخرى في عدد الروبوتات العسكرية عبر "توزيعها نحو 11,000 طائرة مسيرة و12,000 روبوت أرضي في أنحاء العالم". وتتمتع هذه الآلات بعتاد جيد وهي قاتلة، قامت بالفعل بقتل الآلاف. ففي عام 2011 أشارت التقديرات إلى وجود روبوت مقابل كل خمسين جندياً، وبحلول عام 2023، ربما يصبح هناك عشرة روبوتات مقابل كل جندي بشري في الجيش الأميركي.

تساعد المركبات الأرضية غير المأهولة (يو.جي.في)، مثل باكبوت الذي تنتجه آي.روبوت، بشكل روتيني اليوم في الكشف عن أجهزة التفجير المحسّنة (آي.إي.دي) وتعطيلها. وروبوت طالون الذي تنتجه فورستر ميلر هو "روبوت محمول يعمل على سلاسل صغيرة" مثل دبابة مصغرة. ويمكن تزويده ببندقية آلية أو بندقية خمسين مم أو قاذف رمانات أو صواريخ مضادة للدبابات، كل ذلك مع إمكانية التحكم به عن بعد بواسطة مقبض تحكم. أما روبوت ساند فيليا من إنتاج بوسطن داياميكس، فلا يتجاوز وزنه 11 باونداً، وهو قادر على القفز إلى ارتفاع ثلاثين قدماً، بحيث يحط على سطح مبنى أو يقفز بدقة من نافذة مفتوحة ليلتقط كل ما يراه بواسطة الكاميرا العالية الدقة المزود بها. وقد طورت الشركة بيغ.دوغ أيضاً، وهو روبوت رباعي الأرجل قادر على حمل ما يصل إلى أربعمئة باوند من

المعدات والأسلحة والسير بها بسهولة على أرض وعرة متابعاً سيده الجندي بكل طاعة. ويمكن لعربات أرضية أخرى، مثل روبوت رايس، وهو صرصور روبوتي سداسي الأرجل، تسلق الجدران، بينما يمكن لروبوت شيتا الجري بسرعة ثلاثين ميلاً في الساعة تقريباً (أي أسرع من العداء الجامايكي يوزين بولت)، ويمكن لبير رفع وحمل جندي جريح من أرض المعركة، بينما يمكن لرويبت بحجم رسالة من إنتاج آي.روبوت استخدام تقنيات التعرف على الوجوه لتحديد هوية شخص بين حشد من الناس وملاحقته.

وفي السماء، يمكن للطائرات من دون طيار أن تقوم بجمع الصور واعتراض الاتصالات وإطلاق الصواريخ على الأهداف الموضوعة لها. ويمكن لطيارين بعيدين يجلسون في الطرف الآخر من الكرة الأرضية قتل أعدائهم (الذين قد يكونون أبرياء) بنقرة من الفأرة. فوفقاً لبيتر سينجر، وهو خبير مشهود له في الروبوتات العسكرية، ثمة 55 بلداً آخر على الأقل لديها برامج روبوتية عسكرية. وقد أصبحت العربات غير المأهولة جزءاً أساسياً من الترسانة العسكرية، فمن المتوقع أن يصل "الإنفاق العالمي على الطائرات المسيرة، العسكرية منها والمدنية، بالإجمال إلى 89 مليار دولار" بحلول عام 2023. فثمة طائرات مسيرة كبيرة وصغيرة ومروحية وبحجم اليد وعلى شكل حشرة. وتكلف طائرة مسيرة مثل إم.كي.9 ريبر نحو 21 مليون دولار، أي عشر سعر طيارة إف – 22 النفاثة، مع أنها تتمتع بالميزات نفسها تقريباً. ويلاحظ المسؤولون العسكريون أن الطائرات المسيّرة مثل ريبر المذكورة وبريديتر قد تم تصميمها بحيث تتولى تنفيذ "سلسلة القتل" بكاملها على أهدافها العالية القيمة عبر "تحديد الموقع، التتبع، الاستهداف، التنفيذ، والتقييم".

أما طليعة أسطول الطائرات المسيرة فهي غلوبال هاوك. فمع عرض جناحيها البالغ 130 قدماً ووزنها البالغ 32 ألف باوند، يمكنها البقاء في الجو

لمدة يومين على ارتفاع ستين ألف قدم. وليست الحساسات التي يحملها أسطول الطائرات المسيرة أقل إدهاشاً، فهي تشتمل على أدوات مثل أرغوس - إي.إس، الكاميرا الأعلى دقة في العالم والقادرة على التقاط صور بدقة 1.8 غيغابيكسل. وتأتي هذه الكاميرا مزودة بميزة "التحديق المستمر" التي تكافئ مئة طائرة مسيرة من نوع بريديتور، والتي تسمح لها بتتبع أية تحركات أرضية على مساحة تبلغ نصف مدينة كاملة من الحجم المتوسط. وتمتاز الصور التي تلتقطها بجودة عالية، إلى حد أن الطائرة المسيرة تولّد مليون تيرا بايت من البيانات كل يوم، أي ما يعادل خمسة آلاف ساعة تصوير عالي الوضوح (إتش.دي)، تسجل كل تحرك على الأرض (سواء كان سيارة أو حافلة أو شخصاً أو كلباً)، كما يمكنها تشغيل الفيديو مثل مشغل الفيديو الرقمي عند الرغبة.

لكن الأهم هو أن الطيارات المسيّرة قد غادرت منذ وقت طويل مسرح الحرب، وباتت تشاهد اليوم وهي تنفذ مهام مدنية في الوسط القاري للولايات المتحدة، تراقب مهربي المخدرات وعصابات الجريمة المنظمة وعابري الحدود غير الشرعيين. كان المتعهدون العسكريون التقليديون، مثل نورثروب غرومان وبوينغ ولوكهيد مارتن، أوائل الداخلين في عالم الروبوتات، تتبعهم شركات أصغر أكثر تخصصاً مثل بوستن داياناميكس وآي.روبوت (أجل، أولئك نفسهم الذين يصنعون مكنسة رومبا الكهربائية التي تقتنيها يصنّعون أيضاً باكبوت الذي يعطل المتفجرات). لكن لاعباً مشاكساً جديداً قد دخل عالم الروبوتيات، إنه غوغل.

يشن عملاق البحث على الإنترنت حملة شراء روبوتية، حيث اشترى أو استحوذ على ثماني شركات منفصلة تعمل في مجال الروبوتيات في غضون ستة أشهر عام 2014، من بينها شركات متخصصة في الروبوتات السائرة الشبيهة بالبشر والأذرع الروبوتية والبرمجيات الروبوتية والرؤية

الحاسوبية. أما عملية الاستحواذ الأكبر والأكثر مفاجأة فهي شركة الروبوتات العسكرية بوسطن داياميكس، وهي المجموعة نفسها التي طورت بيغدوغ وشيتا وساند فلي ورايس وبيتمان (روبوت شبيه بالبشر يسير على قدمين من الوارد جداً أن يصبح جندي المستقبل). كما زايدت غوغل على عرض فايسبوك لشراء تيتان إيروسبيس التي تصنّع طائرات مسيّرة بحجم الطائرة النفاثة، تعمل بالطاقة الشمسية قادرة على البقاء في الجو لمدة ثلاث سنوات دون أن تحطّ. فلماذا يتصارع عملاقان من عمالقة الإنترنت للتفوق في الجو؟ إنهما تدّعيان أن الطائرات المسيرة يمكن استخدامها لتوفير إمكانية الوصول إلى الإنترنت في أنحاء العالم، التي لا تزال غير متصلة بالشبكة. لكن عندما تدخل إحدى أكبر الشركات في العالم في مجال البيانات والذكاء الصنعي مملكة الروبوتيات، وتصبح قادرة على إطلاق جيوش الطائرات المسيّرة الخاصة بها، فإن أسئلة هامة لا بد من طرحها حول نوايا الشركة وقدراتها.

روبوت في كل بيت، وفي كل مكتب

غرفة معيشتك هي جبهتك الأخيرة أمام الروبوتات.

سيرثيا بريزيل، مخبر الوسائط في معهد ماساتشوستس للتقانة

في مقالة بليغة له في مجلة "سينتيفيك أميريكان"، يقارن بيل غيتس بين الروبوتات الصناعية وحواسب المنصات الكبيرة، متوقعاً أن يسؤدي تصغيرها، إضافة إلى تعميم المعايير التقنية وتوفر حساسات أفضل، إلى إدخالها إلى كل منزل خلال السنوات القادمة. وثمة دلائل تشير إلى أنه على حق. فلدينا منذ اليوم روبوتات منزلية تنظف الأرض وتسقي الزرع وتنظف بعد الشواء وتطعم الحيوانات. وقد باعت شركة آي.روبوت أكثر من عشرة ملايين مكنسة رومبا منذ إطلاقها، وباتت هذه المكانس متوفرة في متاجر وولمارت. يستمتع الأطفال بتجميع أرقام متزايدة من الدمى الروبوتية، مثل

مايندستورم من ليغو أو بوبوسيبيان إكس من وووي، والكرة الروبوتية من سفيرو. وحتى ربة المنزل الاستثنائية مارثا ستيورت اشترت مروحية مسيرة رباعية من نوع دي.جي.آي فانتوم مزودة بكاميرا عالية الوضوح (إتش.دي)، تستمتع بتطييرها حول منزلها النيويوركي الرحب الذي تبلغ مساحته 153 فداناً. أما سوق روبوتات المكتب والمستهلك ففي ارتفاع سريع، والطلب عليها يتنامى أسرع سبع مرات من نمو الطلب على الروبوتات الصناعية.

لا تزال الروبوتات المنزلية حتى اليوم تصنّع لكي تنجز مهمة واحدة، مثل المكنسة الكهربائية. أما في المستقبل، فستصبح لدينا روبوتات متعددة الوظائف قادرة على إنجاز المزيد، مثل تنظيف الطاولة بعد وجبة طعام ووضع الأواني في الجلاية وكيّ القمصان ولملمة الألعاب وراء الأطفال، بينما يتم التحكم بكل ذلك بسهولة عبر شاشات الهواتف النقالة المألوفة لدينا. وصحيح أن مساعِدات منزل الأحلام هذه لم تصبح واقعاً بعد، وربما يتطلب تحقيقها أعواماً، إلا أن التقدم جار على قدم وساق. وقد نجحت حملة على إنديغوغو قادتها الدكتورة كينثيا بريزيل من معهد ماساتشوستس للتقانة، في جمع الأموال لتطوير روبوت اجتماعي ذكي يدعى جيبو قادر على التعرف على أفراد الأسرة والتقاط صور عائلية وقراءة البريد الإلكتروني وقص الحكايات قبل النوم على الأطفال، وتغيير تعابير وجهه للتعبير عن العواطف. ويستطيع روبوت بي.آر.2 بالفعل طيّ الملابس وإحضار جعة من البراد والتنظيف وراء الكلب وخبز الحلويات وتحضير إفطار كامل. ومن اليابان إلى أوروبا والولايات المتحدة، ثمة مبالغ غير مسبوقة من الدولارات تتدفق في مجال الروبوتيات.

لا بد من الاعتراف بأن بعض هذه التطورات تبدو وكأنها قادمة من إحدى روايات فيليب كي.ديك. فجليسة الأطفال الروبوتية على سبيل المثال باتت

موجودة اليوم في كوريا الجنوبية واليابان. وهي قادرة على لعب الألعاب وإجراء محادثات محدودة باستخدام تقنيات التعرف على الكلام. وكثيرون يستخدمون عيني الروبوت لنقل تصوير حي للأطفال إلى الحاسب أو الهاتف الذكي. وتسمح لك بابيرو، جليسة الأطفال الروبوتية من نيك، أيضاً بالتحدث مع أطفالك مباشرة عبر الرسائل النصية التي تقوم الروبوتة بقراءتها على أطفالك، وتدعي شركة سوفتبانك أن روبوتها بيبر يستطيع "أن يقرأ مشاعر أطفالك وتعابير وجههم بحيث يستجيب بالشكل المناسب". ومع أن جليسات الأطفال الروبوتية قد تثبت فائدتها بالنسبة للآباء المثقلين بالمهام والمحرومين من النوم في كل مكان، فإن مجالاً آخر للروبوتات الشخصية يشهد تنامياً أكبر بكثير هو روبوتات العناية بالمسنين. فنظراً للتغيرات الديمغرافية وشيخوخة الشعوب في الدول المتقدمة في أنحاء العالم، ثمة ندرة في كوادر الرعاية القادرة على تقديم الدعم المادي والمعنوي الذي يحتاج إليه المسنون. وما من مكان تصعب فيه هذه المهمة كاليابان، حيث تبلغ نسبة السكان الذين بلغوا الخامسة والستين 25 بالمئة. فللمساعدة على التخفيف من المشكلة، خصصت حكومة شينزو آبي مبلغ 2.39 مليار ين عام 2013 للمساعدة على تطوير روبوتات العناية بالمسنين محلّياً. مثال ذلك بارو، وهو روبوت دمث ظريف مهمته مصاحبة المسنين. ويمكن لبارو "التعرف على أصوات الأفراد المختلفة وتتبع الحركات وتذكر السلوكيات التي تثير ردود فعل إيجابية لدى المرضى". فعند ملامسته، يستجيب بارو بالهديل وبمعانقة الشخص الذي يلمسه. وقد تم بيع الآلاف من وحدات بارو عالمياً، وأثبتت فائدتها الكبيرة مع مرضى الخرف في خفض مستويات العنف وتحسين المزاج. ومع إدراكها لحاجة السوق إلى روبوتات رعاية المسنين، افتتحت آي.روبوت (مُصنّعة المكانس الكهربائية الروبوتية والروبوتات القاتلة) قسماً جديداً خصيصاً لخدمة المسنين.

من أكثر أنواع روبوتات رعاية المسنين نمواً روبوتات الحضور عن بعد، أي تلك الآلات التي تسمح للناس بـ "الانتقال افتراضياً في أرجاء بناء بعيد عبر التحكم عن بعد بروبوت مزود بعجلات وميكروفون ومكبرات صوت وشاشة لعرض الفيديو الحي" لوجه الشخص الذي يتحكم بالروبوت عبر الإنترنت. وتسمح روبوتات مثل مانتاروبوت وجيراف بلس من إي.يو للأطفال بـ "الإشعاع" من بعد آلاف الأميال، لتوجيه روبيت على عجلات له وجه أشبه بجهاز آيباد اللوحي بهدف التواصل مع المسنين. فيمكن للأقارب تفقد أحبائهم من المسنين وتناول وجبة طعام معهم عبر محادثات مصورة تشبه محادثات سكايب، بل حتى التأكد من أنهم قد استيقظوا أو من أنهم لم يسقطوا على الأرض في شققهم. وليس البالغون القلقون الوحيدين الذين يستخدمون روبوتات الحضور البعيد لتفقد آبائهم، فهم بدورهم يحصلون على إقامة طويلة في المشفى. وتسمح روبوتات آر.بي – فيتا (مساعِدات الحضور البعيد للطب الافتراضي المستقل عن بعد) للأطباء، خصوصاً منهم الاختصاصيين، بالظهور إلى جانب مرضاهم وتشخيص حالتهم دون أن يكونوا موجودين مادياً في الغرفة نفسها بالضرورة. فبضغطة زر على الآيباد، يمكن لطبيب موجود في الطرف الآخر من المدينة أو من الكرة الأرضية أن يوجّه روبوتاً إلى جانب المريض ويقرب الصورة عبر التحكم ببؤبؤ الروبوت، بل أن يجعل ممرضة تضع سماعة على صدر المريض لكي يستمع إلى نبضات قلبه. ويبقى السؤال القائم هو ما إذا كانت الروبوتات أحسن سلوكاً في عيادة المرضى.

بدأت الشركات بدورها تدرك قيمة وجود روبوتات حضور بعيد في المكتب، تسمح للموظفين بتجريد حضورهم المادي بواسطة أجهزة يتم التحكم بها عن بعد. فلدى شركات مثل سوتَبل تيكنولوجيز ودوبل روبوتيكس نماذج تبلغ كلفة الواحد منها نحو 3000 دولار تسمح للموظفين

بالعمل من المنزل، بينما تتجول أرواحهم الروبوتية في أروقة مكاتبهم أو تصعد إلى زملائهم في مكاتبهم أو تصيخ إلى جميع الشائعات الجديدة في غرفة الطعام. وحتى مسرّب وكالة الأمن القومي الشهير إدوارد سنودن استخدم رويبتاً للحضور البعيد ليقدم عرضاً أمام آلاف الحاضرين في مؤتمر تيد في فانكوفر عام 2014، دون أن يضطر إلى مغادرة أمان مخبأه السري في روسيا.

يرجى من البشر عدم التقدم للوظيفة

سنشهد مع الوقت ظهور الروبوتات في كل مهنة وفي كل مهمة قد تخطر لنا. فقد أدخلت فنادق ستاروودس بالفعل نادلين روبوتيين "مستعدين ليل نهار". وهي قادرة على إيجاد طريقها إلى أية غرفة من غرف النزلاء وإيصال فرشاة أسنان نسيها أحدهم أو خدمة تم طلبها، تاركة لكادر الفندق مزيداً من الوقت للاهتمام بمهام أخرى. ويستطيع رويبت البرغر من مومينتوم ماشينز إنتاج 360 هامبرغر محضّرة بإتقان كل ساعة، مع وضع الإضافات (الخس والكاتشب والبصل) وفق طلب الزبون بمنتهى الدقة.

أجرت دراسة لجامعة أوكسفورد حول مستقبل العمل تحليلاً مفصّلاً لأكثر من سبعمئة مهنة عام 2013، وخلصت إلى أن 47 بالمئة من الموظفين في الولايات المتحدة مهددون إلى حد كبير بخسارة فرص عملهم لمصلحة الأتمتة الروبوتية بحلول عام 2023. ويواجه أولئك الذين يعملون في مجال النقل (أي سائقو سيارات الأجرة والحافلات وشاحنات الطرق الطويلة وسائقو فيديكس وسائقو توصيل البيتزا) خطراً أعلى مما يواجه غيرهم، فاحتمال استبدالهم في أعمالهم بعربات آلية يبلغ 90 بالمئة. لكن فرص العمل المتدنية المستوى ليست وحدها في خطر. إذ تستخدم منافذ الأخبار، مثل الأسوشييتيد بريس ولوس أنجلوس تايمز، برمجيات روبوتية وخوارزميات قادرة على كتابة آلاف المقالات، حول مواضيع تتنوع من الصراعات والزلازل

إلى أحدث المكاسب في مجال الأعمال. فالعينات يمكن "تحليلها بفعالية أكبر بواسطة برمجيات معالجة الصور مقارنة بتقنيي المختبر"، ويمكن لبرمجيات كويك بوكس تنفيذ معظم المهام التي يقوم بها محاسب. ويعتقد كثيرون أن تنامي الأتمتة والروبوتيات هو الذي قاد إلى الركود العميق في الأجور الذي نشهده منذ عام 2004. فقد كان بيل غيتس متبصراً في تنبؤاته حول مستقبل الروبوتيات وحضور الروبوت في كل بيت ومكتب. لكن سواءٌ كان عملك هو تقليب الهمبرغر أم قيادة شاحنة أم كتابة أحدث الأخبار، فإن كل من قرأ أو شاهد "كروم الغضب" لجون ستينبيك يعلم أن الانتقال سيكون قاسياً على أولئك الذين بقوا في المؤخرة.

حتى التعهيد الخارجي بات اليوم يستبدل بالتعهيد الروبوتي، مفوتاً فرص العمل على البشر سواءٌ محلياً أم وراء البحار. فمع ازدياد ذكاء الآلات وقدراتها، قد ينعم الجنس البشري بنهضة مدهشة يتم فيها إنجاز جميع المهام اليومية الرتيبة من قبل الروبوتات، ما يفسح لنا المجال للاستمتاع بالراحة مع وقت فراغ غير محدود، يمكننا فيه الغناء والرقص والرسم بينما نشمّس عضلاتنا الضامرة على أحد الشواطئ. في المقابل، قد ينحدر المجتمع في الفوضى مع تمرد الجماهير غير العاملة وغير المؤهلة للعمل على القلة من القياصرة البشر المتحكمين بروبوتات العالم. وسيكون الاتجاه الذي تتحول فيه مجريات الأحداث منوطاً بما نتخذه اليوم من قرارات سياسية وقانونية واقتصادية وأخلاقية.

حقوق الروبوتات وقوانينهم وأخلاقياتهم وخصوصياتهم

الإنسان بلا أخلاق ليس سوى وحش شارد على هذه الأرض.

ألبير كامو

بينما لن يدافع أحد عن ضرورة شمل مكنسة رومبا الروبوتية بالإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة، فإن ازدياد ذكاء

الروبوتات وربما وعيها في المستقبل البعيد، سيؤدي بلا شك إلى طرح مثل هذه الأسئلة. وحتى ذلك الوقت، ستجلب الروبوتات إلى عالمنا جملةً من المسائل السياسية والقانونية والأخلاقية التي لن يتوقف تأثيرها على القوة العاملة. فإذا ثقب روبوت جراح شريان مريض مؤدياً إلى وفاته، فهل يمكن للعائلة المنكوبة أن تقاضي الروبوت أو مُصنّعه بسبب الخطأ المهني؟ وعندما تتورط سيارة ذاتية القيادة في حادث، هل من الممكن أن تكون مذنبة؟ وهل يمكن مقاضاة الراكب الذي لا يقود فيها؟ أو شركة السيارات؟ أو الشركة التي طورت برمجيات القيادة والملاحة؟ إذا كان من الواضح أن العربة الذاتية القيادة ستكون طرفاً في اصطدام لا مناص منه، فهل على خوارزمية الاستجابة المثلى للاصطدام الخاصة بها أن توجهها بحيث تصطدم بعمود الهاتف (متسببة بمقتل الراكب)، أم براكب الدراجة النارية على ميسرتها أم بسيارة الشيفروليه على ميمنتها، أم بالراجل الذي أمامها؟ مع أن قدراتنا على بناء الروبوتات وتوظيفها تتنامى بمعدّل أسي، فإننا أخلاقياً ما زلنا نحبو.

مع أن علائم الانتشار الشامل للروبوتات باتت تلوح في الأفق، ثمة ندرة في علماء الأخلاق وخبراء السياسة والمشرّعين المدركين لخصوصية الروبوتات، والقادرين على مواكبة الأسئلة المعقدة التي ستطرحها هذه التقدمات العلمية على البشر. وسنشهد على وجه الخصوص اعتداءات جديدة لم يكن من الممكن تخيلها في السابق على خصوصيتنا. فتماماً كمواقع الوسائط الاجتماعية والتطبيقات والهواتف النقالة قبلها، ستأتي الروبوتات مع شروط خدمة تورد تفاصيل الشروط التي تؤمن الحماية لمصنّعي الروبوتات وتؤثر على خصوصيتك. ومع أن مكنستك الروبوتية أو رويبت العناية بالمسنين أو الدمية التي لديك تجلس في ركن الغرفة، وقد بدت عليها البراءة والظُرف مستعدةً للخدمة بإشارة منك، فإنها مدجحة بمجموعة من الكاميرات

والميكروفونات والحساسات القادرة على رؤية وتسجيل كل شيء تقوم به ضمن خصوصية منزلك.

تمثل طائرات الهواة المسيّرة المزوّدة بكاميرات عالية الدقة منذ اليوم تهديداً على خصوصيتنا لم نعهده من قبل. ففي منتصف عام 2014، فوجئت شابة في سياتل تسكن شقة في الطابق السادس والعشرين، برؤية طائرة مسيرة رباعية (وهي طائرة مروحية صغيرة مزودة بأربع مراوح) تحوم قبالة نافذتها تماماً وتصورها وهي تغير ملابسها في غرفة النوم، إنه تحقيق لفيلم "توم المتلصص" في القرن الحادي والعشرين. وفي حادثة أخرى في سياتل، قرر رجل أن يحوم بطائرته المسيرة الخاصة المزودة بكاميرا فوق حديقة جاره. وعندما سمعت امرأة الصوت، والذي ظنّته صوت جزّازة عشب، فتحت ستارة نافذة غرفة نومها في الطابق الثاني لتتفقد ما يجري، لتُفاجأ بطائرة مسيرة تحوم أمام النافذة على بعد بضعة أقدام. وعندما أرسلت زوجها ليتحرى الأمر، وجد جاره يوجّه الطائرة، وعندما طلب من قائد الغزو الروبوتي التوقف عن التصوير في الحال، رفض الأخير مدعياً أن من حقه قانوناً أن يصور. وقد يكون محقاً في ذلك.

بينما يعتبر السير على مرجة أحدهم انتهاكاً لحرمة الملكية، فإن التحليق بمروحية (سواءٌ كانت صغيرة أم كبيرة) ليس كذلك كما يستنتج من قرار المحكمة العليا العائد لعام 1946، والذي نص على أن "السماء هي طريق مشاع". وقد وقع عناصر الشرطة الذين استُدعوا إلى الموقع في هذه الحوادث في سياتل في حيرة من أمرهم بالطبع، ولم يكونوا الوحيدين في ذلك. فوفقاً لتقرير محكمة يعود إلى عام 2012 ويتناول التحليق بالطائرات المسيّرة في الولايات المتحدة، خلص مكتب المحاسبة الحكومي إلى أنه "ما من هيئة فدرالية اليوم تمتاز بالاختصاص القانوني لتشريع مسائل الخصوصية المتعلقة بنظم الملاحة الجوية غير المأهولة للحكومة الفدرالية

ككل. ونظراً إلى قدرة هذه الأجهزة على حمل كاميرات ذات قدرات كبيرة وحساسات أشعة تحت حمراء ومعدات للتعرف على الوجوه وقارئات للوحات السيارات، فإن البعض يرون في هذه الطائرات المسيرة تهديداً كبيراً على الخصوصية". حقاً؟

ليست هذه القضايا التي تثار حول من يملك حقوق الجو فوق الملكيات ومَن يمكن تصويره وأين سوى بداية البداية لمجموعة في غاية التعقيد من المسائل القانونية والأخلاقية والسياسية العامة، التي لا شك ستبرز أكثر بكثير مع تكاثر أعداد الروبوتات العاملة في مجتمعنا. وربما تعود أول محاولة للتعامل مع هذه الأسئلة الأساسية إلى عام 1942، عندما نشر إسحق أزيموف قصته القصيرة "الهارب"، والتي صاغ فيها مصطلح "الروبوتية" وقدم فيها قوانينه الروبوتية الثلاثة الشهيرة:

1. لا يحق لروبوت أن يؤذي الإنسان أو أن يسمح بتقاعسه لإنسان بالوقوع ضحية الأذى.
2. على الروبوت أن يطيع أوامر بني البشر إلا إذا كانت تتعارض مع القانون الأول.
3. على الروبوت حماية وجوده طالما كانت هذه الحماية لا تتعارض مع القانونين الأول والثاني.

بينما يعطينا أسيموف نقطة بدء ممتازة نتأمل من خلالها في هذه القضايا، فإننا لم نكن قادرين في ذلك الوقت على بناء آلة تفهم بدقة معنى كلمة "إفطار"، ناهيك ببنية مجردة مثل "الأذى". ستحتاج الروبوتات على الأرجح إلى قواعد أخلاقية أكثر مرونة وتكيفاً، لكننا حتى اليوم لم نقترب مجرد اقتراب من مثل هذه القواعد. إلا أن نزعتنا إلى نشر الروبوتات الصناعية والعسكرية والطبية والشخصية على نطاق واسع لا تتوقف، ولا بد للحوادث من أن تطرأ.

ثمة خطر يا ويل روبينسون

"ثمة خطر يا ويل روبينسون!" هي العبارة التي كثيراً ما كان يرددها الروبوت الحارس على مسمع المغامر الفضائي الصغير، محذراً الصبي من أخطار تحيق به في المسلسل التلفزيوني "تائه في الفضاء" في الستينيات. وليت جميع الروبوتات تتخذ مثل هذه الاحتياطات في تعاملها مع البشر. فمع ازدياد تعامل البشر مع الروبوتات، ثمة تبعات غير متوقعة، ليس أقلها الإصابات الخطيرة أو حتى الموت على أيدي هذه الآلات، حتى تلك منها التي يفترض أن تساعدنا. ففي عام 2013، أطلقت إدارة الغذاء والدواء تحقيقاً في كثير من الحالات التي تسبب فيها الروبوت الطبي دافنشي من إنتاج إنتيويتيف سورجيكال بالأذى، وهي حوادث يقال إن الشركة لم تبلغ بها الحكومة كما ينص القانون. ففي إحدى الحالات، أصيب رجل بثقب في الكولون خلال عملية بروستات، وفي حادثة أخرى، قبض الروبوت على نسيج داخلي للمريض رافضاً إفلاته، على الرغم من محاولات الجراح البشري فتح قبضة يد الآلة. ولم يتخلَّ الروبوت عن قبضته إلى أن تمت إعادة تشغيله. وفي حادثة أخرى أيضاً، تعرضت امرأة إلى لطمة في وجهها من قبل روبوت خلال عملية استئصال للرحم.

تحدث الغالبية العظمى من الإصابات الناجمة عن التفاعل بين البشر والروبوتات ليس مع الروبوتات الجراحية بل مع تلك الصناعية. وعلى الرغم من غياب إحصاءات شاملة لحوادث الروبوتات على مستوى العالم، كثيرة هي التقارير عن مثل هذه الحوادث. ففي عام 2007 على سبيل المثال، اقترب عامل من روبوت لإصلاحه معتقداً أنه قام بقطع الطاقة عن الآلة. لكن الطاقة كانت لسوء الحظ لا تزال موصولة، فعاد الروبوت فجأة إلى الحياة، وقبض على الرجل من رأسه ورفعه عن الأرض، وانكسرت أربعة من أضلعه قبل أن يتمكن من أن يحرر نفسه بعد جهد. عند التصادم بين

الآلة والإنسان، من المرجح أن تكسب الآلة، وكثيرة هي الحالات التي انتهت بالموت. وقد حدثت إحدى أوائل حالات القتل التي ارتكبها روبوت عام 1981، عندما كان موظف يدعى كينجي أورادا في السابعة والثلاثين من عمره في شركة كاوازاكي للصناعات الثقيلة، يعمل على إصلاح روبوت لم يكن قد أطفأه بشكل كامل. فمع عدم قدرة الروبوت على استشعار الرجل، اصطدمت ذراع الروبوت الهيدروليكية به خطأً وأسقطته في آلة طحن مجاورة ليقضي على الفور. ونعود إلى الولايات المتحدة، حيث قُتل عامل في معمل سيارات عام 2001 عندما دخل إلى قفص روبوت غير مقفل لتنظيفه. فما كان من الآلة، التي اعتقدت أن الرجل قطعة من سيارة، سوى أن تناولت الرجل من رقبته وأحكمت قبضتها عليه إلى أن مات خنقاً. ووفقاً لإدارة الصحة والسلامة المهنية، فقد وقع ما لا يقل عن 33 حادثة وفاة في الولايات المتحدة وحدها، وهو رقم مرشح للزيادة مع خروج الروبوتات من أقفاصها وبدئها بالعمل بيننا، إذ لا يبدو أن على هذه الروبوتات أن تستمع إلى السيد أزيموف وقوانينه الثلاثة.

تصبح الحوادث الروبوتية أسوأ بكثير عندما يرى أحدهم أن تزويد الروبوتات بأسلحة آلية هي فكرة جيدة، كما اكتشف عناصر قوة الدفاع الوطني الجنوب أفريقية عام 2009 خلال تدريبات بالذخيرة الحية. فقد تعرض مدفع أورليكون إم.كي.5 مزدوج مضاد للطيران يتحكم به حاسب، إلى خطأ برمجي واضح جعله يطلق النار في وضعية آلية تماماً بمعدل 550 رشقة في الدقيقة وهو يدور حول نفسه في جموح، دورات كاملة كأنه خرطوم مياه منفلت في حديقة. وعندما انتهى الأمر، كان تسعة جنود، من بينهم العديد من الضباط الإناث، قد لقوا مصرعهم بينما جرح أربعة عشر آخرون جروحاً بالغة، مخلفين مشهداً دموياً يذكر فيلم "الفاني". إنها حادثة تبين أنه عندما تضرب روبوتاً "شاشة الموت الزرقاء" الحاسوبية، يمكنه أن

يتسبب بالموت وأن يحدث آثاراً عميقة في فضائنا المادي الثلاثي الأبعاد. وليست الروبوتات الصناعية أو الأرضية هي الوحيدة التي قد تخطئ، بل تلك الطائرة منها أيضاً.

وفقاً لتقرير لواشنطن بوست، سبق لأكثر من أربعمئة طائرة مسيّرة عسكرية أن سقطت من السماء عن طريق الخطأ محلياً أو خارجياً "مرتطمة بمنازل ومزارع ومدرجات وطرق سريعة، بل وبطائرة نقل عسكرية من طراز هرقل سي - 130 أثناء تحليقها في أحد الحوادث". أما عدم موت أحد في أي من هذه الحوادث المبلّغ عنها، فهو معجزة حقيقية. ففي عام 2009، فقد قائد طائرة ريبر مسيّرة عرض جناحيها 66 قدماً السيطرة عليها، لتنفلت طائرة عبر أفغانستان. ولم يتوقف الروبوت الطائر المتمرد سوى عندما تدخلت مقاتلات نفاثة أميركية وأسقطته قبل أن يدخل الأجواء الطاجيكية.

وعودةً إلى الديار، فقد تحطمت نحو خمسين طائرة مسيرة في الولايات المتحدة، بما فيها طائرة مسيرة تابعة للجيش يبلغ وزنها 375 باونداً، سقطت على الأرض بجوار مدرسة ابتدائية في بنسلفانيا "بعد دقائق فقط على انصراف التلاميذ إلى منازلهم". لكن الحوادث الروبوتية تبقى الاستثناء، فحدوثها نادر نسبياً، وثمة مبادرات إجرائية تتخذ لتزويد الروبوتات بأنظمة تتوقع الاصطدامات وتتجنبها لمنع الكثير من الحوادث الصناعية. إلا أنه نظراً للنمو الهائل الذي نتوقعه في أعداد الروبوتات المنزلية وروبوتات موقع العمل والمصنع والروبوتات الطبية والحربية، فإن الخطر أبعد ما يكون عن البساطة، وهو خطر سيزداد إلى حد كبير مع انضمام الروبوتات إلى إنترنت الأشياء وإمكانية اختراقها عن بعد من قبل عناصر خبيثة.

اختراق الروبوتات

في المستقبل، عندما تترك مايكروسوفت ثغرة أمنية في شيفرتها البرمجية،

فلن تكون النتيجة أن يخترق أحدهم حاسبك، بل سيؤدي ذلك إلى سيطرة أحدهم على خادمك الروبوتي ليقف على باب غرفة نومك وهو يشحذ سكيناً ويراقبك وأنت نائم.

دانييل إتش. ويلسون، عالم روبوتيات وكاتب

ثمة العشرات من أنظمة التشغيل الخاصة بالروبوتات، معظمها احتكارية، تدير كل شيء، من أنظمة الأسلحة العسكرية إلى نظم سكادا للتحكم الصناعي. لكن ما يحدث في الحواسب المحمولة والهواتف الذكية من تجمّع حول بضعة نظم تشغيل متصدرة، ينطبق أيضاً على الروبوتات التي تستخدم نظام روس، أو نظام التشغيل الروبوتي. الأمر الذي سيكون له أثر إيجابي هائل على مستقبل الروبوتات نظراً لعدم اضطرار المبرمجين إلى إعادة اختراع العجلة في كل مرة يريدون فيها برمجة وظيفة جديدة في روبوت. ونظام روس مجاني ومفتوح المصدر ويوفر وحدات للمحاكاة والحركة والرؤية والتنقل والفهم والتعرف على الوجوه، وغيرها من الوظائف الروبوتية. وهذه المبادرات التي تقوم بها جماعات المصدر المفتوح التي تقوم على المشاركة، والتي كنا بالكاد نسمع بها قبل بضع سنوات، هي بالذات ما يمكّن شركات من مثل ريثينك روبوتيكس من عرض روبوت باكستر بسعر 22 ألف دولار بدلاً من 200 ألف.

يخضع روس، الذي تم تطويره في الأصل في شركة ويلو غاراج عام 2007، لإدارة منظمة الروبوتيات المفتوحة المصدر اليوم، وهو قادر على تشغيل كل شيء، من الدمى الصغيرة إلى الروبوتات الصناعية الضخمة. وكما نوهنا مرات عديدة في هذا الكتاب، فإننا لم نعرف حاسباً لا يمكن اختراقه بعد، والأمر نفسه ينطبق على الروبوتات أيضاً، وستكون له آثار كبيرة على أمننا المشترك. فمهمة المخترقين ستصبح، من دون أن يتعمد ذلك أحد، أسهل بوجود نظام تشغيل روبوتي قياسي يمنحهم هدفاً موحداً يهاجمونه. ومن

شأن تقييس نظام روس شامل أن يعبد الطريق أمام هجمات سايبرية على نطاق واسع، تماماً كما شاهدنا مع الحواسب الشخصية. ومن الهام أن ننوه إلى وجود فارق جوهري بين اختراق الروبوتات واختراق أنظمة الحوسبة الأخرى أو غيرها من الأغراض على إنترنت الأشياء: فالروبوتات تتنقل بشكل دائم في فضائنا المادي، فهي تسير وتقود السيارة وتركض وتطير وتسبح في كل مكان حولنا. ويمكن اختراق الروبوتات المتصلة بالإنترنت وإعادة توجيهها بطرق كثيرة خطيرة وخبيثة، وهي حقيقة لم تفت المجرمين ولا الإرهابيين. فعندما يخترق هؤلاء الروبوتات، لن يتمكنوا من استخدام حساساتها للتجسس وحسب، بل سيصبح بوسعهم استخدام محركاتها وأذرعها وأرجلها وعجلاتها للملاحقة والضرب والدفع وإطلاق النار والطعن والجر والقتل.

ليست الروبوتات في جوهرها سوى حواسب متحركة، حواسب ستحرر الجريمة السايبرية من قضبان الشاشات الثنائية الأبعاد، وتطلق يدها في عالمنا المادي اليومي. وقد قام باحثون في جامعة واشنطن بتفحص ثلاثة روبوتات منزلية، من بينها إيريكتر سبايكي وروبوسابين وروفيو من ووويي، وكشفوا عن ثغرات أمنية خطيرة في كل منها، منها تسرب كلمات السر وسوء تحقيق وظائف التشفير أو غيابها كلّياً، ما يعني أنه بإمكان طرف ثالث الاستيلاء على الأجهزة عن بعد وتحريكها وتسجيل الصوت والفيديو بواسطتها. ووصف الباحثون الجانب الأمني في هذه الأجهزة بأنه "مجرد ملحق". لكن مع ازدياد انتشار الروبوتات في مجتمعنا وتنقلها في عالمنا، فإنها ستنضم إلى مليارات الأغراض المتصلة بإنترنت الأشياء. وكما رأينا سابقاً، فإن عشرات الآلاف من أنظمة المكالمات الفيديوية الجماعية المستخدمة في وكالات المحاماة والشركات الدوائية والمراكز الطبية، تعاني نقصاً عميقاً في الأمن وقد تم اختراقها بنجاح، فحتى قاعة اجتماعات

غولدمان ساكس لم تسلم من ذلك. فلماذا ستكون روبوتات الحضور البعيد، وما هي إلا أجهزة مكالمات فيديوية متنقلة، مختلفة في ذلك؟ تستطيع هذه الروبوتات أن تسير خلفك في أنحاء المكان وتنصت، أو أن تجلس في مكان ما بصمت خلال الاجتماعات مراقِبة كل شيء. إنها أدوات ممتازة للتجسس الصناعي. وعندما يغلق معملك وتطفأ الأضواء، يمكن للقراصنة من الطرف الآخر للكرة الأرضية أن يسيطروا على الروبوتات ويسيّروا مفاصلها. فربما يكون لديك حارس يمنع اقتراب المجرمين، لكن هؤلاء ربما كانوا يقبعون في البناء سلفاً.

تطرح إمكانية اختراق الروبوتات العديد من الأسئلة الهامة. فما مدى الخصوصية التي يحققها روبوت الرعاية الصحية الذي يقدمه طبيبك عبر الإنترنت؟ والأسوأ من ذلك هو أن الروبوتات الصناعية التي تحضّر الهامبرغر وتقطع الطماطم ستكون مسلحة بالسكاكين الحادة، فكيف نعلّمها توخي الحذر حين تكون على مقربة من البشر؟ على الرغم من توفر أنظمة سلامة لدى معظم الروبوتات الصناعية كما رأينا، فإن الحوادث قد تطرأ، وبعضها قاتل. وإجراءات السلامة الروبوتية مرمّزة في برامج حاسوبية، ويمكن للمخترقين من المبرمجين التدخل في هذه الإجراءات وتعطيلها. ومن الوارد جداً أن تتعرض الأجيال القادمة من الروبوتات المنزلية القوية إلى إساءة الاستخدام بطرق لم تكن لتخطر على بال مصمميها. وتماماً كما يقوم مستخدمو الهواتف الذكية اليوم بتحرير هواتف الآيفون للتخلص من القيود البرمجية المزعجة، فإنهم سيفعلون الشيء نفسه مع روبوتاتهم، ما يفتح الباب أمام مجموعة من سيناريوهات "الروبوتات المستوحشة".

لنأخذ مثلاً هجوماً على طريقة "إنما إيماننا بالشاشات"، يقوم فيه عامل بإطفاء الروبوت قبل تنظيفه كما تنص التعليمات، بينما يكون مهاجم قد

تدخل في الروبوت وتركه في حالة عمل. وبينما تظهر الشاشة أن الروبوت بأذرعه الصناعية الضخمة مطفأ، فإن العامل غير المدرك لما يجري، والذي يقترب من الجهاز، سيجد نفسه وقد التُقِط من رقبته ورفع منها إلى أن يقضي اختناقاً. إنها طريقة عظيمة للتعامل مع زميل العمل الذي لم يرقك في القسم 3 – ب. أما بقية العالم، فربما يبدو لها الأمر مجرد حادث عمل آخر. وإذا بدت مثل هذه السيناريوهات مبالغاً فيها، فثمة بالفعل أدلة على اختراق بعض أكثر الروبوتات حماية في العالم، أي روبوتات الجيش والشرطة.

لعبة الطائرات المسيّرة

> عليك أن تبقي الطائرات المسيّرة تحت السيطرة، عليك وضع قواعد معينة للاشتباك لمنع أو لتخفيف الإصابات الناتجة. إنه أمر في غاية الأهمية.
>
> فلاديمير بوتين

في أواخر عام 2009، مع استعار الحرب في الشرق الأوسط، كانت طائرات بريديتر الأميركية المسيرة تطير على نحو شبه دائم في سماء العراق. وكانت مهامها تتنوع، من جمع المعلومات الاستخبارية إلى "تنفيذ العمليات الحركية ضد أهداف عالية القيمة"، مثل إطلاق صواريخ هيلفَيَر (نار الجحيم) ضد المتمردين. وكان قادة الطائرات الذين ينفذون هذه العمليات عن بعد على مسافة سبعة آلاف ميل من صحراء نيفادا، يشاهدون بثاً حياً يعرض لهم أهدافهم بينما يوجّهون طائراتهم المسيّرة وراء طرائدهم. إلا أنه تبين لاحقاً أنهم ليسوا الوحيدين الذين يشاهدون البث. فقد توصلت الميليشيات الشيعية إلى طريقة لاختراق الأسطول الأميركي الروبوتي الطائر والتقاط بثه الفيديوي الحي. فباستخدام برمجية اختراق

روسية تعرف باسم سكاي غرابر، تكلّف 26 دولاراً، عادة ما تباع في الأوساط السرية الرقمية لسرقة إشارات التلفزة الفضائية، كان المتمردون قادرين على استقبال البث الفيديوي السري الصادر عن طائرات بريديتور المسيرة. أي إنه بينما كان الأميركيون يراقبون المتمردين، كان هؤلاء يراقبونهم بدورهم، ما منحهم تفوقاً تكتيكياً ومعلومات استخبارية حاسمة على أهدافهم من الحلفاء. فحين كانت الميليشيات تشاهد بناءً لها يتم التقريب عليه بالفيديو، كانت تعلم أنه قد حان الوقت للتفكير ببناء جديد تلجأ إليه.

لم تكن تلك بالتأكيد هي المرة الأولى التي يتم فيها اختراق طائرة مسيرة بنجاح، فقد سبق أن حدث ذلك حتى على الأراضي الأميركية. إذ تستخدم وزارة الأمن الداخلي أسطولاً من هذه الطائرات المسيرة لحماية الحدود، لتكتشف عام 2012 أنها لم تكن محميّة على الإطلاق كما كان يعتقد. فقد اكتشف طلاب من جامعة تيكساس في أوستين طريقة لاختراق الطائرات المسيرة وحاولوا إعلام الوزارة، التي رفضت تصديقهم قائلة إن الطائرات "غير قابلة للاختراق". وبعد أشهر من الأخذ والرد، اقتنع المسؤولون أخيراً بحضور عرض يقدمه الطلاب. وقام الطلاب المبدعون من جامعة تيكساس في هذا العرض بالسيطرة على إحدى الروبوتات الطائرة وبدأوا بتوجيهها بحيث تخرج عن مسارها بانعطافات حادة، تاركين المسؤولين من وزارة الأمن الداخلي فاغري الأفواه. أما الطلاب فقد نفذوا هجومهم عبر تزوير إشارات نظام الموقع الجغرافي التي تستقبلها الطائرة المسيرة وتغيير موقعها، وذلك كله باستخدام تجهيزات وبرمجيات قاموا ببنائها في الجامعة بتكلفة لم تتجاوز الألف دولار. أما أستاذهم، تود هومفريز (الرجل نفسه المسؤول عن اختراق أنظمة الموقع الجغرافي على اليخت الفائق وايت روز أوف دراكس الذي ذكرناه سابقاً)، فقد علّق بذكاء على الحادثة قائلاً إنه "خلال

خمس إلى عشر سنوات سيكون لدينا 30,000 طائرة مسيرة تجوب الأجواء الوطنية... يمكن لكل منها أن تتحول إلى صاروخ يوجّه صوبنا".

انتبه آخرون إلى الأمن، ومن بينهم الإيرانيون، الذين نجحوا في استخدام التقنية نفسها لتعطيل خطوط اتصالات طائرة الآر.كيو 170 سينتينيل الأميركية المسيرة التي كانت تحلق في بلادهم، وأجبروها على التحول إلى وضعية الطيار الآلي. فقامت الطائرة باتباع التعليمات المبرمجة فيها والعودة إلى قاعدتها في أفغانستان، أو هذا ما كانت تظنه على الأقل. أما الحقيقة، فهي أن الإيرانيين قد نجحوا في تزوير إشارات نظام الموقع الجغرافي للطائرة المسيرة وتوجيه الجندي الروبوتي إلى أيدي الحرس الثوري الإيراني مباشرة. وكان أسر الطائرة المسيرة وتقانتها السرية ضربة استخبارية كبيرة للإيرانيين ودليلاً جديداً على أن عصر اختراق الروبوتات قد حلّ. وليست الطائرات المسيّرة نفسها هي كل ما يمكن اختراقه، بل كذلك أنظمة تحكمها وتوجيهها. ففي عام 2011، ضرب فيروس حاسوبي قوي أسطول الطائرات المسيرة الأميركي مصيباً قمرة الطيار في طائرات بريديتور وريبيتر الأميركية، مسجّلاً كل مفتاح يضربه الطيارون وهم ينفذون مهامهم بالتحليق فوق أفغانستان. وبقي مصدر الاختراق غير معروف حتى أواخر عام 2014، حيث لا يزال الحادث قيد التحقيق.

وفي عام 2013، شرح القرصان المتسلسل سامي كَمكَر (ونشر الشرح على الإنترنت ليستغله الآخرون) هجوماً سمح له بتوجيه طائرة مسيّرة خاصة به، بحيث تلاحق روبوتات طائرة أخرى في السماء وتخترقها وتحولها إلى جيش روبوتي مادي من الطائرات المسيّرة تحت إمرته. وتقوم البرمجية، التي سمّيت سكاي جاك، باختراق الاتصالات اللاسلكية الشبيهة باتصالات الهاتف الذكي التي تتحكم بالطائرة المسيرة، مثل وحدة باروت إيي.آر واسعة الانتشار، والتي عادة ما تباع في متاجر كوستكو، للسماح للمهاجمين بتوجيه

نظم التصوير والتحكم بالطيران على الطائرة المسيرة الضحية. وقد تم بيع أكثر من 500,000 طائرة مسيّرة مزودة بوحدات باروت هذه، وتقنية كمكر قادرة على خطف مثل هذه الطائرات المسيرة، كتلك التي ستتولى بلا شك توزيع البضائع في مدننا خلال السنوات القادمة، وستتمكن من إعادة توجيه جميع الطرود ووجبات البيتزا بالزمن الحقيقي. يبدو مستقبل الجريمة الروبوتية واعداً بالفعل، وقد بدأت شركات الجريمة بتخصيص موارد كبيرة لهذا الغرض.

روبوتات سيئة السلوك

عام 1982، وفي شوارع بيفرلي هيلز الفاخرة في كاليفورنيا، اعتقلت الشرطة مجرماً غير اعتيادي هو روبوت دي.سي - 2، كان يوزع مناشير إعلانية بشكل غير قانوني في حي الأعمال في المدينة دون تصريح. وعندما اقترب الضباط من الروبوت الضال السائر على عجلات والبالغ ارتفاعه أربع أقدام، وجدوا أمامهم آلة تحمل شاشة قديمة ولوحة مفاتيح على الصدر ولها رأس شبيه بخوذة رائد الفضاء. وعندما طلب رجال الشرطة من مشغّل الروبوت الغامض التعريف بنفسه، فوجئوا بسيل من الشتائم ينهال عليهم من مكبرات الصوت المركبة على الروبوت. وحاول رجال الشرطة، الذين لم يجدوا ذلك مضحكاً، تفكيك الروبوت والحجز عليه، لكن الروبوت حينها بدأ بالصراخ بصوت عالٍ أمام الحشد الذي تجمع حولهم "ساعدونا! إنهم يحاولون تقطيعي!". وأخيراً، تم "اعتقال" الروبوت ونقله إلى قسم الشرطة بواسطة شاحنة قطر. وبعد ذلك بساعات، ظهر جين بيلي، صاحب الروبوت الذي كانت قيمته 30,000 دولار ومؤسس شركة أندرويد للترفيه، أمام رجال الشرطة جارًّا ولديه المراهقين من أذنيهما. وكان الولدان قد أخذا الروبوت الاحترافي في "نزهة مرح" دون إذن والدهما. ومع أن الشرطة فكرت في تقديم بيلي إلى المحكمة بسبب الحادثة، فإنها في النهاية أطلقت سراح

الروبوت بتعهّد منه. وعندما أجرت وكالة أسوشييتيد بريس مقابلة مع بيلي بعد وصوله إلى منزله، عبر عن سروره باستعادة روبوت دي.سي - 2، مضيفاً "لقد شعرنا وكأن أحد أفراد الأسرة كان في السجن". ربما كان دي.سي - 2 هو الأول، لكنه بالتأكيد لن يكون آخر روبوت يتعرض للحبس.

مع مرور الوقت، سيتم استخدام الروبوتات في سرقة المصارف وعمليات السطو في الشوارع بل وحتى في الخطف. وقد طور القراصنة بالفعل روبوت آر2.بي2، آلة الضغط على الأزرار القابلة لإعادة البرمجة، القادر على تجريب كلمات السر على هواتف آيفون وأجهزة أندرويد المسروقة أو المفقودة بشكر متكرر بمعدل محاولة واحدة في الثانية. وكانت تكلفة بناء الروبوت لا تتجاوز الخمسين دولاراً، فهو يتكون من بعض المحركات وإبرة بلاستيكية وكاميرة ويب "تراقب شاشة الهاتف لتكتشف ما إذا تم اختراق كلمة سر الهاتف بنجاح" (فحتى المجرمون سيستخدمون الروبوتات لأداء المهام المتكررة أو المملة). يمكن للروبوتات أن تكون أفضل صديق للمجرمين، كما اكتشفت شرطة تايوان في منتصف عام 2014، عندما حاولت اعتقال تاجر مخدرات مسلح معروف كان قد حصّن منزله تحصيناً محكماً بواسطة سلسلة من روبوتات المراقبة التي تبث الفيديو، بحيث تعطي إنذاراً مبكراً في حال حضور الشرطة.

كما رأينا في افتتاحية هذا الفصل، فإن الإرهابيين يستخدمون بدورهم الروبوتات كأسلحة، وما بحوزتهم يتجاوز مجرد طائرات مسيّرة من تلك التي تباع للمستهلكين مع سعة تحميل صغيرة. ففي كل من العراق وأفغانستان، تحول الإرهابيون إلى أجهزة الفيبايد (الأجهزة الانفجارية المرتجلة المحملة على عربة)، والشائعة تسميتها بالسيارات المفخخة، لتفجير عدة مبانٍ ودك أحياء بأكملها، مع حمولات للسيارات تصل إلى سبعة آلاف باوند من المتفجرات. فأجهزة الفيبايد هي أسلحة فعالة وقد

سبق لها تدمير الكثير من الأهداف في أنحاء العالم، من بينها أبراج خبر في السعودية وثكنة البحرية الأميركية في بيروت وبناء مورا الفدرالي في أوكلاهوما سيتي.

أما اليوم، فيلجأ الإرهابيون إلى الأسلحة الروبوتية كبديل عن أجهزة الفيبايد السابقة. ففي فيديو تم اكتشافه على الإنترنت، يمكن رؤية مهندسين متلفحين الكوفيات من أنصار الإسلام، يتبجحون بقدراتهم التقنية وهم منحنون يلحمون لوحات دارات حاسوبية. وفي المشهد التالي من المقطع ذي الدقائق الأربع، تشاهَد شاحنة بيك - أب وهي تسير في وسط الصحراء، وقد حمّل عليها رشاش آلي على ثلاث قوائم. ومع تقريب الكاميرا، يتضح أنه ما من سائق في القمرة التي كان يجري التحكم بمحتوياتها عبر أدوات روبوتية بسيطة مركبة على المقود وعلى الدواسات. وما هي إلا لحظات حتى تُسمع رشقات عديدة من الرشاش الآلي، حيث كان محرّك روبوتي يدار عن بعد يضغط على زناد الرشاش.

باستخدام مثل هذه الأنظمة، لن يعود الجهاديون بحاجة إلى الاستشهاد. وسيبقى بمقدورهم العودة للقتال في يوم آخر. ثمة في السلطة التنفيذية من تفطن لإمكانية الاستغلال الإجرامي للمركبات الذاتية القيادة، وقد أصدر مكتب التحقيقات الفدرالي تقريراً داخلياً يعبر عن مخاوفه من استخدام هذه المركبات في المستقبل كأسلحة فتاكة، ويتنبأ المسؤولون في التقرير باستخدام عربات النقل الروبوتية كأجهزة فيبايد مبرمجة، بحيث تقود نفسها آلياً عبر المدينة وتنفجر في الأهداف الموضوعة لها. والأفلام التي تصور مخاوفنا من الروبوتات القاتلة مثل "عالم الغرب"، و"الجاري على الشفرة"، و"الشرطي الروبوتي"، والفاني، و"أنا، الروبوت"، قد تكون لسوء الحظ في المراحل الأولية للتحول إلى حقيقة.

هجوم الطائرات المسيّرة

الطائرات المسيرة مخيفة. لا يمكنك استخدام المنطق مع طائرة مسيرة.

مات غرونينغ

عندما أعلن جيف بيزوس، المدير التنفيذي لموقع أمازون، في أواخر عام 2013 أن "متجر كل شيء" العالمي سيبدأ قريباً باستخدام الطائرات المسيرة الرباعية لتوصيل الطرود إلى زبائنه، قعد العالم مصغياً للخبر. وقام آخرون بالطبع بتوجيه ضرباتهم إلى بيزوس كالمتعهدين الذين أطلقوا مشروع تاكوكوبتر لتوصيل سندويشات التاكو وبوريتو بومبر لتوصيل سندويشات البوريتو بإسقاطها من الجو، ناهيك بالفندق الذي يوصل طلبات الشمانيا لنزلائه إلى جانب بركة السباحة بواسطة الطائرات المسيرة في فيغاس، لكن إعلان بيزوس كان مختلفاً. فقد وصلت أمازون إلى حد من الكمال من الناحية اللوجستية، جعل الطائرات المسيرة تقطع الميل الأخير إلى الزبائن ما سيغير شروط السوق بلا شك. ففي خريف عام 2014 بدأت غوغل بنجاح بتوصيل البضائع تجريبياً بواسطة طائرة وحيدة الجناح بعرض خمس أقدام. ويمكن لطائرة غوغل المسيرة، المسماة مشروع وينغ، الطيران في نطاق عشرة أميال من المستودع لتوصل أي شيء، من السكاكر إلى طعام الكلاب. ولهذه الطائرة محركات تمكنها من الحوم فوق منزل الزبون على ارتفاع مئة قدم، لتنزل إليه المنتجات إلى الأرض بواسطة رافعة ذات حبل قبل أن تحلق عائدة إلى مكاتب الشركة. وثمة بلا شك الكثير من التعقيدات، التقنية والتنظيمية، التي لا بد من العمل عليها في ما يتعلق بهذه الخدمات، لكن الصفقة قد تمت بشكل أو بآخر، فسواءٌ راقك الأمر أم لا، لقد أصبحت حقبة الطائرات المسيّرة التجارية والمدنية حقيقة قائمة.

على الرغم من ربطها في معظم الأحيان بالجيش والتسليح، فإن الطائرات المسيرة قد تكون أيضاً قوة للخير. إذ تستخدم الطائرات المسيّرة في القبض على الصيادين في أفريقيا ولمساعدة المزارعين على العناية بمحاصيلهم في

أميركا. وكانت تستخدم في معاينة الأضرار في موقع كارثة فوكوشيما النووية، كما قدمت المساعدة بعد زلزال هاييتي. أما اليوم، فتقوم الطائرات المسيرة بتعقب العواصف لتوفير إنذارات مبكرة للأعاصير، وتقوم بإطفاء الحرائق وإيصال الأدوية إلى القرى النائية. ويستخدمها وكلاء العقارات لتصوير الملكيات، ويقوم آباء، مثل باول واليش من فيرمونت، بالتحليق بالطائرة المسيرة الرباعية فوق أطفاله وهم يسيرون نحو موقف باص المدرسة المحلية للتأكد من وصولهم بأمان. بل إن شرطة الخيالة الكندية الملكية قد استخدمت طائرة مسيرة رباعية لتصوير أول حالة إنقاذ حياة باستخدام طائرة مسيّرة، حين حلقوا بها فوق منطقة نائية في ساسكاتشيوان لتحديد موقع رجل مصاب مفقود تاه ولم يعد يعرف موقعه، بعد أن تعرضت سيارته لحادث وخرجت عن الطريق في درجات حرارة صقيعية.

ها هو عصر الطائرات المسيرة قد جاء وباتت مواقع الويب مثل دي.آي.واي.درونز تؤسس تجمعات هواة كبيرة، متخصصة في بناء الطائرات المسيرة الشخصية. فقد أصبحت الطائرات المسيّرة سهلة المنال بالنسبة للمستهلكين والشركات والحكومات لا تكلف النماذج البسيطة منها سوى بضع مئات من الدولارات، وتأتي مزودة بحساسات متطورة مثل الكاميرات العالية الدقة التي يمكن استقبال بثها على الهواتف النقالة للمستخدمين. وعلى الرغم من ازدياد شعبية الطائرات المسيّرة ومن إمكانية استخدامها لأهداف خيّرة، فإنها تجلب معها جملة من المخاوف التي تجاوز مسائل الخصوصية التي أتينا عليها في ما سبق. فسرعان ما ستكتظ سماؤنا بهذه الأجهزة، وسنتوق ذات يوم إلى الأيام الخوالي التي كان بإمكاننا فيها النظر إلى الأعلى لرؤية السماء خالية من حجافل الطائرات المسيّرة الرباعية، التي تجرّ وراءها شرائط بيبسي وفياغرا وكوبرتون حين يتنامى حقل "الإعلان بالطائرات المسيّرة". وسيزداد الطين بلّة حين تتلاقى إمكانات تحليل

البيانات الكبيرة مع الروبوتيات. فحينها، بدلاً من أن ترى الإعلانات على شريط في متصفح الوب مختارة وفقاً لتاريخ عمليات البحث التي أجريتها وبيانات المتصفح وإعجاباتك على الفايسبوك، ستظهر الطائرات المسيّرة التي تحمل إعلانات موجّهة أمام نافذتك أو ستتبعك في الشارع وهي تحمل لوحات إعلانية حقيقية. كما أن وجود المزيد من الروبوتات يعني المزيد من الحوادث. فإذا كان وارداً أن تسقط من السماء 400 طائرة مسيّرة يقودها طيارون عسكريون مدربون، فما الذي سيحدث حين يبدأ أطفال مخمورون باللعب بهذه الطائرات في حفلة طلابية؟

إذا كان بإمكان مارثا ستيوارت أن تجد طريقة لجعل طائرتها المسيّرة تطير فوق ملكيتها العقارية وتصورها، فبإمكان المجرمين فعل ذلك أيضاً. ولن تستخدم الطائرات المسيّرة المزودة بالكاميرات في أشياء بديهية مثل التجسس الصناعي واستطلاع المواقع تحضيراً للسطو فقط، بل قد تصبح أيضاً عوناً للأزواج الغيورين والزوجات الغيورات في تعقب طلقائهم، في حالات ربما تشتمل على عنف عائلي أيضاً. كما أن القراصنة قد وجدوا طرقاً لاستخدام الطائرات المسيّرة بهدف استقبال الاتصالات، سواءٌ بالتنصّت على اتصالاتك الهاتفية أو بتتبع كل حركة تقوم بها على الإنترنت مع توفر أجهزة مثل واسب (منصة المراقبة الجوية اللاسلكية).

ومنصة واسب التي تم الكشف عنها في لاس فيغاس عام 2011، هي عبارة عن طائرة صغيرة يبلغ عرض جناحيها ست أقدام ويتم التحكم بها عن بعد. وتحمل المنصة أحد عشر هوائياً، وهي مزودة بتشكيلة من أدوات الاتصالات والحساسات، بما فيها كاميرا عالية الوضوح. وقد تم تصميم الواسب بحيث تطير فوق الحي وتستقبل جميع إشارات الواي - فاي في الجوار، حتى تلك الخاصة بالشبكات المشفّرة. وتحمل الطائرة حاسب لينوكس صغيراً يشغّل مجموعة من أدوات الاختراق، بما فيها قاموس

مخصص يحتوي على 340 مليون كلمة يمكن للطائرة المسيّرة استخدامها، لتوليد كلمات مرور وتجريب جميع الإمكانات لدخول شبكتك بالزمن الحقيقي. كما تحمل طائرة الواسب برجاً خلوياً منتَحلاً يمكنها استخدامه لـ "تقمّص" مقدم خدمة جي.إس.إم للهواتف النقالة. إذ يقوم البرج الخلوي المنتحل باستدراج هاتفك للاتصال بطائرة الواسب والسماح للقراصنة بتسجيل جميع مكالماتك الهاتفية ورسائلك النصية التي تمر عبر الجهاز. كانت مثل هذه القدرات الاستخبارية في مجال الإشارات تكلف عشرات الملايين من الدولارات قبل وقت ليس بالطويل، ولم تكن متاحة سوى لأكثر جيوش العالم تقدماً. أما طائرة الواسب فكانت تكلفة بنائها 6000 دولار.

مع هذه التكلفة الزهيدة للطائرات المسيّرة المزودة بكاميرات عالية الدقة، بدأت تظهر في أماكن كثيرة لم تكن متوقعة من قبل، مثل مواقع الاحتجاجات وأعمال الشغب. ففي وارسو ببولندا أطلق متظاهرو حركة "احتلّوا" طائرة رباعية لتوثيق نشاطات شرطة مكافحة الشغب العنيفة وهي تحاول ضبط الآلاف باستخدام غاز الدموع. وكانت الطائرة، التي سميت أُكيو - كوبتر (أو احتلوكوبتر)، تطير على ارتفاع مئة قدم مزوِّدةً المحتجّين بصور نقية إلى حدّ مذهل، تبين ضباط الشرطة وهم يتحركون في رتل محاولين تطويق المظاهرة، فأصبحت أداة فعالة لم يكن من الممكن تخيلها من قبل، لمواجهة الرقابة، في أيدي البشر العاديين. ومن نافل القول إن رجال الشرطة لن يكونوا الوحيدين الذين سيرتبكون في استجابتهم لطائرات مسيرة تحوم فوق رؤوسهم.

تلجأ الجريمة المنظمة إلى الروبوتات الطائرة كوسيلتها المفضلة لتهريب الأسلحة والهواتف الخلوية والمخدرات إلى الإصلاحيات في أنحاء العالم. ففي مركز ساو خوسي دوس كامبوس للحبس الاحتياطي في ساو باولو بالبرازيل،

شاهد ضباط الإصلاحية طائرة رباعية مسيرة تطير فوق أسوار السجن وتُسقط حزمة صغيرة في باحة السجن الترفيهية، ليكتشفوا أنها تحتوي 250 غراماً من الكوكايين. وفي ضواحي موسكو كانت مروحية يتحكم بها عن بعد هي التي أوصلت 700 غرام إلى داخل سجن تولا. أما في اليونان، فكانت الشحنة عبارة عن صندوق من الهواتف النقالة. وثمة حوادث مشابهة لاقتحام السجون في كندا وأستراليا والولايات المتحدة. فالجريمة المنظمة تعمل بهدوء على بناء أسطولها الجوي الروبوتي.

من المهم التنويه إلى أن الطائرات المسيّرة المستخدمة في الجريمة لا تتوافق البتة مع المنهجيات الأمنية المتوفرة لدينا حالياً. إذ تعتمد السجون على أسوار عالية مدببة، غالباً ما تكون مكهربة لعزل المجرمين لأسباب تتعلق بالسلامة العامة، وقد بقي هذا النظام فعالاً نسبياً على مدى مئات السنين. لكن آليات الأمن والدفاع لدينا معدّة بحيث تدافع عنا في وجه المجرمين البشريين وليس في وجه أولئك الروبوتيين. ربما حان وقت إعادة التفكير في ذلك، فالطائرات المسيّرة قادرة لا على تجاوز أسوار السجون وحسب، بل أي سور آخر، بما في ذلك السور الذي يحيط بحديقتك وببناء مكتبك، بل حتى بالحدود الوطنية، كما بينت عصابات المهربين في أميركا اللاتينية. ففي المكسيك على سبيل المثال، وظفت عصابات الجريمة المنظمة عمال خط التجميع من معامل الطيارات المحلية، لكي يسهروا الليل لتصميم الطائرات المسيّرة لمصلحة هذه العصابات. وفي منطقة سانتا في في مكسيكو سيتي، في جوار معمل مومباربير تماماً، تم اكتشاف معمل طائرات مسيرة إجرامية وفقاً لأمانة الأمن العام المكسيكية. وهذه الطائرات المستقلة الخفيفة جداً، والمبنية اعتماداً على تصاميم أميركية وأوروبية وإسرائيلية، أكبر بكثير من الطائرة الرباعية الاعتيادية وتزن مئة باوند ولها جناحان قابلان للطي بحيث يمكن نقلها بسهولة مخبّأة في شاحنات على أي من جانبي الحدود.

وهي تطير على ارتفاعات منخفضة ولا يمكن كشفها بواسطة الرادار. ويمكن لكل واحدة منها حمل مئة كيلوغرام من الكوكايين في كل رحلة تقوم بها، وهي كمية من المخدرات تصل قيمتها إلى 1,700 دولار للكيلو في كولومبيا و8000 دولار في المكسيك و30,000 دولار في الولايات المتحدة، ما يجعل الربح الصافي للمهرّبين أكثر من مليوني دولار للرحلة الواحدة. ومنذ عام 2 قام قسم مكافحة المخدرات بتوثيق ما لا يقل عن 150 عملية عبور لطائرة مسيرة، عائدة للعصابات حملت ما مجموعه عدة أطنان من الكوكايين. وبتحقيق أرباح كهذه، تعيد العصابات، من كالي إلى سينالوا، استثمار عائداتها في المزيد من عمليات البحث والتطوير المتقدمة منفقة الملايين لضمان دور أكثر هيمنة لقواتها الروبوتية الإجرامية المتقدمة.

وبعيداً من المخدرات، ثمة الكثير من المواد الإشكالية التي يمكن لخبراء الجريمة تحميلها على الطائرات المسيّرة، بما فيها الأسلحة. واليوتيوب يعج بالفعل بالهواة الذين يستعرضون روبوتات طائرة يدوية الصنع يتم التحكم بها عن بعد، وتنفّذ مهام متقدمة مثل تتبع الأشخاص وتصويب أسلحة مائية أو قنابل ألوان عليهم، وهي أدوات تسلية مثالية يمكن للمجرمين أو الإرهابيين تكييفها لأهدافهم. وثمة مقاطع فيديو أخرى تظهر هواةً وقد حمّلوا طائرات مسيّرة بصاعقات كهربائية وهم يطلقون الشحنات الكهربائية على فرائسهم مركعينها أرضاً بشحنة كهربائية تصل إلى ثمانين ألف فولت. لكن الأمور لا تقف عند ذلك الحد، بل لقد استخدمت الأسلحة الحقيقية أيضاً. ويعود أول فيديو يظهر سلاحاً حقيقياً إلى عام 2008، وكان السلاح عبارة عن مسدس 45 - كاليبر مركب على متن مروحية تحكم عن بعد. ومنذ ذلك الوقت، ظهرت على الشبكة مقاطع أخرى كثيرة تعرض طائرات مسيّرة يتحكم بها بواسطة الهاتف الذكي محملة بالأسلحة، بما فيها فيديو بدقة عالية يعرض طائرة رباعية تحمل مسدس كولت 45 وهي

تطلق النار عدة مرات بواسطة إصبع روبوتي على الزناد يتحكم به عن بعد. وبوجود ما يسمى تقانات "اتبعني"، يمكن لهذه الطائرات أن تتتبع فرداً معيناً تتبعاً مستقلاً وهو يركض في الشارع. وباستخدام الهاتف الذكي لإطلاق النار من بندقية حقيقية مركبة على الطائرة، يعلن الروبوت الطائر الذي لا تتجاوز كلفته مئات الدولارات دخول ألعاب تصويب الشخص الأول في الفضاء الثلاثي الأبعاد وتحولها إلى حقيقة. فهل سيمر وقت طويل قبل أن يقوم مجرم أو شخص مختلّ عقلياً باستخدام هذه الأجهزة لقتل أحدهم؟

ربما بدا مثل هذا السيناريو خطيراً ومرعباً، إلا أن حمولات أخرى أكثر خبثاً قد يتم تحميلها على متن الطائرات المسيّرة أيضاً، بما فيها المتفجرات بل حتى أسلحة التدمير الشامل، كالأسلحة البيولوجية والكيماوية والإشعاعية. فمقابل أقل من عشرين دولاراً، يمكن الحصول عبر الإنترنت على أنظمة إلقاء قنابل للطائرات بعيدة التحكم، تشبه نوافذ إلقاء القنابل في الطائرات العسكرية التي تفتح بالتوجيه عن بعد أو عند الوصول إلى نقطة جغرافية معينة. فهل ستصبح الطائرات المسيّرة هي الجيل القادم من الطائرات الانتحارية؟ لدى القاعدة ومنظمة لاشكار - إي - طيبة والكثير من المنظمات الإرهابية الأخرى برامج نشطة لتطوير الطائرات المسيرة. وثمة الكثير من مقاطع الفيديو على اليوتيوب التي تظهر مزارعين، وقد أعياهم العمل في القيظ، حولوا مروحيات التحكم عن بعد التي لديهم إلى طائرات زراعية. لكن إذا استغل إرهابي الفكرة نفسها لبخّ مواد قاتلة على حشد من البشر بدلاً من رشّ المبيدات الحشرية على حقول الأرزّ، وسيكون حجم الضرر المحتمل بالغاً.

يمكن استخدام الطائرات المسيّرة، كما بيّن لنا الجيش، بأسلوب دقيق التوجيه لاستهداف أفراد بعينهم، سواءٌ لثأر شخصي أو كهجوم إجرامي أو إرهابي. وقد بدأنا بالفعل نشهد تعرض شخصيات هامة لاعتداءات غريبة

وخطيرة في آن معاً. ففي أواخر عام 2013، وجدت المستشارة الألمانية أنغيلا ميركل نفسها عرضة لهجوم طائرة مسيرة، حين انقضت عليها وهي على المنصة طائرة رباعية خلال حملة انتخابية في دريسدن لتتحطم عند قدمها. ونفذ الهجوم حزب القراصنة الألماني الذي صرح بأنه كان يريد أن يتأكد من أن المستشارة تدرك "كيف يكون الأمر حين تخضع إلى المراقبة بواسطة طائرة مسيرة". ولا شك في أن حرسها الأمني قد تلقى الرسالة. فعلى الرغم من أن أحداً لم يصب بأذى، كان يمكن أن تكون نهاية الحادثة نهاية غير سعيدة لو أن الجهاز كان مسلّحاً أو محمّلاً بالمتفجرات.

كما يمكن للطائرات المسيّرة إحداث الضرر عند إطلاقها على وسائل نقل أخرى، بحيث تحدث صدمة لدى سائقي العربات وتؤدي إلى تصادمهم. وثمة بالفعل الكثير من التقارير عن هواة في أنحاء العالم يوجهون طائراتهم المسيّرة عمداً إلى مسار طيران طائرات نفاثة دافعين بالطيارين إلى القيام بمناورات عنيفة تجنباً للاصطدام، كما حدث مع الخطوط أميريكان إيرلاينز ويو.إس إيرويز والإيطالية وفيرجين بلو. ولو شُفِط أي من هذه الروبوتات الطائرة من قبل محركات الطائرة لتسبب بسهولة في حادث تحطم على غرار الحادث الذي سقطت فيه طائرة نفاثة تعود إلى خطوط يو.إس إيرويز في نهر هودسون بالقرب من نيويورك. ومع مرور الوقت ودخول الروبوتات الطائرة والسابحة والدارجة والسائرة في حياتنا، يترتب علينا إيجاد طرق تسمح لنا بالعيش إلى جانبها بسلام وأمن، لكن مستقبل الروبوتيات نفسها قد يجلب معه مخاطر أكبر بعد لا بد من إدارتها.

مستقبل الروبوتيات والآلات المستقلة

ستصبح الروبوتات أسرع وأصغر وأكثر ذكاءً. وثمة تطورات عظيمة تتحقق منذ اليوم في مجال الروبوتات الصغرية. ويتم توجيه هذه الأجهزة، التي يبلغ ببعضها الصغر أن يتسع له رأس إصبعك، عن بعد ويمكن تزويدها

بكاميرا عالية الدقة وميكروفون، ما يدفع بمسائل الخصوصية إلى مستوى جديدٍ تماماً. فطائرات دراغونفلاي المسيّرة استخدمت، وفقاً للتقارير، منذ عام 2007 للتجسس على المحتجين المعارضين للحرب في واشنطن العاصمة، كما كشفت القوى الجوية عن نحلات طنانة روبوتية لا يمكن كشفها في البيئات المعادية بينما تطير إلى المباني لـ "تصوير الإرهابيين وتسجيل أصواتهم بل ومهاجمتهم".

ثمة تطور آخر يحدث اليوم في مجال الروبوتيات ويتمثل في القدرات "السربية"، أي النظم المتعددة الروبوتات التي تتصرف كوحدة لها سلوكها المشترك الذي يحاكي طريقة تعاون النمل أو أسراب الطيور. فباستخدام قدرات حاسوبية متقدمة موزّعة لحل المسائل وللتنظيم الذاتي، يمكن لأسراب الروبوتات أن تنسق جهودها لتحقيق أهداف لا تصدق، سواءٌ في التخفيف من آثار الكوارث، أو في البحث والإنقاذ، أو في حالات تسرب النفط أو في التصنيع. وثمة تقدمات كبيرة يتم تحقيقها في مجال الذكاء السربي، ففي منتصف عام 2014 نجح باحثون في جامعة هارفارد في تطوير أكبر سرب روبوتي على الإطلاق، مستعينين بـ 1024 روبوتاً صغيراً بحجم بنس يمكنها العثور على بعضها والتعاون لتجميع نفسها في تشكيلات وتصاميم مختلفة، كشكل نجمة أو أشكال حروف أبجدية، كأنها حشد مفاجئ ميكانيكي. لكن هذه الأسراب ربما تشير أيضاً إلى عاصفة تلوح في الأفق، فالروبوتات المتعاونة القادرة على تنظيم نفسها قد تستخدم أيضاً للشر. فإذا كانت طائرة مسيرة محمّلة بمسدّس تلاحقك في الشارع فكرة سيئة بما فيه الكفاية، فلا شك في أن سرباً مؤلفاً من ثلاثين من هذه الطائرات سيكون مرعباً ومن غير المحتمل أن تنجو منه. علاوة على ذلك، ومع انتشار استخدام الروبوتات السربية، فإن أي اختراق تتعرض له أو فيروس يصيبها سيكون كارثياً، فهو سيؤثر على جميع الروبوتات في الشبكة،

تماماً كما تصور لنا مشاهد المسلسل التلفزيوني ستار تريك، حين يستخدم طاقم يو.إس.إس إنتربرايز فيروساً حاسوبياً ينجح في تدمير تجمع بورغ للمتعضيات السايبرية، باستثناء أننا نحن من سيكون هدف التدمير. وعندما يبدأ الجيش باستخدام الطائرات المسيّرة المسلحة التي تعمل في أسراب لمهاجمة الأعداء ويحدث أن يصيب فيروس هذه الطائرات (كما سبق أن حدث لطائرة مسيرة أميركية قيادية)، ما مدى سهولة قلب الروبوتات الطائرة المسلحة على أسيادها أو توجيهها ضد السكان المدنيين الأبرياء؟

علاوة على ما سبق، سنجد أنفسنا محاطين لا فقط بروبوتات صغيرة تحلق حولنا في أسراب، بل بآلات أكثر استقلاليةً أيضاً قادرة على تنفيذ المهام واتخاذ القرارات في العالم الحقيقي بمفردها دون تحكم صريح من الإنسان. فالروبوت المستقل، مثل مكنسة رومبا الكهربائية، يتخذ القرارات بناء على برمجته، لكنه يتخذها بنفسه وبالزمن الحقيقي مستخدماً خوارزميات "اصطدم وتابع" للتحرك وتفادي العقبات، ما يمكنه من تحليل بيئات لم يعتدها والتأقلم معها.

إلا أن الأسئلة الصعبة بحق في ما يتعلق بالاستقلالية، تبرز مع الروبوتات العسكرية. فمتى يتم تجاوز الحد؟ فالطبيب العسكري الروبوتي الأرضي، الذي يستطيع أن ينقذ جندياً جريحاً من أرض المعركة وتقديم المساعدات الأولية التي قد تنقذ حياته، قد يبدو فكرة عظيمة. أما طائرة مسيرة قادرة على إيجاد هدفها واتخاذ قرار إطلاق النار بهدف القتل بشكل مستقل فقد تدفع الكثيرين إلى التردد. إلا أن هذا هو بالتحديد ما ينتظرنا على طريقنا، فمع تقدم الروبوتيات والذكاء الصنعي وسرعات المعالجة الحاسوبية وتحسنها بمعدّل أسي، سنصل إلى نقطة يعجز عندها البشر بسرعتهم عن المواكبة، وخصوصاً في مجال التسلّح. فحين ينتقل عدونا إلى الأسلحة

المستقلة تماماً، ستكون مجبراً على فعل الشيء نفسه للحيلولة دون دمارِك.

ومع أنها تذكر بأفلام نهاية العالم المتشائمة، كالفاني، فإن الآلات القاتلة المستقلة موجودة بالفعل. فنظام بي.إيي.إي تارانيس يشتمل على طائرة مستقلة تماماً قادرة على "الطيران إلى عمق مناطق العدو لجمع المعلومات الاستخبارية وإلقاء القنابل والدفاع عن نفسها ضد الطائرات المعادية المأهولة وغير المأهولة". وفي المنطقة منزوعة السلاح التي تقسم شبه الجزيرة الكورية، نشرت كوريا الجنوبية الروبوتات القناصة إس.جي.آر - 1 من سامسونغ لخفر الحدود واكتشاف المتسللين بواسطة حساسات حرارية وحركية لتطلق النار آلياً على الأهداف الواقعة على مسافة تصل إلى كيلومتر واحد من بنادقها الألية المدمجة بعيار 5.5 مم وقاذفات الرمانات من عيار 4 مم. ومع أن الروبوتات الحدودية تتطلب اليوم إذناً بشرياً لتنفيذ الهجوم وفقاً لما تنص عليه سياسة نشرها، فإنها تقنياً قادرة على التحول إلى الاستقلالية التامة بمجرد قلب بدّالة إلكترونية. ستتخذ الروبوتات القاتلة المستقلة الكثير من الأشكال، فستكون آلات تسير وتسبح وتطير وتقود وهي تطارد فرائسها أو ستقعد متربصة بها. لكن على الرغم من قدراتنا التقنية المتنامية التي تسمح لنا بإيكال قرارات القتل إلى الآلات، فإن فعل ذلك سيفرض جملة من المضاعفات القانونية والأخلاقية والمعنوية والأمنية.

ربما تكون حوادث الروبوتات الصناعية مؤلمة، لكن الحوادث التي تتورط فيها روبوتات مزوّدة بأسلحة آلية، كما تبين لنا حادثة حاسب قوى الدفاع الوطنية الجنوب - أفريقية، قد تكون كارثية. ومع انتشار الروبوتات، سنعاني التبعات التي ستنجم عن التقاء قانون مور بقانون مورفي. البرمجة السيئة، والبيانات غير الدقيقة والأخطاء البرمجية ستؤدي بلا شك إلى مأساة حين يكون بمقدور الروبوتات أن تقرر القتل بنفسها. علاوة على ذلك، ستكون الروبوتات المسلّحة المتصلة بالإنترنت قابلة للاختراق، كما

بروتوكولات وميزات الأمان فيها، ما يضيف خطراً إضافياً لا بد من التفكير به. وينطبق الأمر نفسه على الحكومات المستبدة التي تستخدم الروبوتات القاتلة لقمع المتمردين أو عصابات المخدرات التي تقتل رجال الشرطة وعصابات المخدرات المنافسة. وقد يبدو من المبالغ فيه اليوم تخيل أن يكون للجريمة المنظمة روبوتاتها القاتلة الخاصة، لكن ذلك سيحدث بالطبع، تماماً كما سبق لها أن تبنّت عدداً من التقانات العسكرية المتفوقة الأخرى، بما فيها مناظير الرؤية الليلية والإنترنت والطائرات المسيّرة. يساور القلق حيال إيكال قرارات القتل للآلات الخبراء في مجال حقوق الإنسان وفي التقانة على حد سواء. كما تمت إثارة الموضوع من قبل الأمم المتحدة وهيومان رايتس ووتش ومنظمات جديدة مثل اللجنة الدولية لضبط تسليح الروبوتات وحملة وقف الروبوتات القاتلة. بل إن مؤلف الخيال العلمي دانييل سواريز وعالم الروبوتيات نويل شاركي، قدما عروضاً تقديمية مثيرة حول الموضوع في مؤتمر تي.إي.دي منادين بحظر عالمي للروبوتات التي تقتل البشر أو تؤذيهم، وهي فكرة معقولة بالفعل، كما اقترح أزيموف لأول مرة قبل عقود.

ما من شك في أن الروبوتات ستدخل حياتنا من كل باب، من رعاية المسنين إلى تحضير الطعام والجراحة. وهي قد تشكّل قوة هائلة للخير. لكن كما رأينا عبر هذا الفصل، يمكن استخدام الروبوتات أيضاً من قبل عصابات الشوارع والمتلصصين وعصابات المخدرات والإرهابيين، ولا شك في أن هذه النزعة ستتواتر مع تحسن وظائف الروبوتات وتراجع أسعارها، وخصوصاً مع التقانات الجديدة المكملة التي لا تصدق، مثل الطباعة الثلاثية الأبعاد.

طباعة الجريمة: عندما يلتقي غوتنبرغ بغوتي

من الصعب فرض القيود في عالم يمكن فيه لأي شخص أن يفعل أي شيء.

هود ليبسون

تَعِد الطباعة ثلاثية الأبعاد، والتي تسمى أحياناً بالتصنيع التراكمي، ببعث الحياة في جهاز النسخ المعروف في مسلسل ستار تريك. فبضغطة زر، يمكن لآلة سحرية أن تصنع أغراضاً مادية أمام عينيك باستخدام مجموعة من المواد، من بينها اللدائن والمعادن والخشب والإسمنت والسيراميك، بل وحتى الشوكولا. فتماماً كما ترسل صورة إلى طابعة نفث الحبر ثنائية الأبعاد، يمكنك أيضاً أن تحمّل أو تنشئ تصميماً على حاسبك وترسله إلى الطابعة الثلاثية الأبعاد التي يمكنها، بتطبيق عدة تقنيات، أن تبني الأغراض بأبعاد ثلاثية، طبقة تلو الأخرى، بدقة مدهشة. وبفضل هذه التقنيات الرقمية التصنيعية تتراجع صعوبة وتكلفة بناء لا الروبوتات وحدها بل طيف عريض من المنتجات، من قطع تغيير الطائرات إلى الكاميرات المفردة العدسة القابلة للاستخدام والعدسات.

نوه غولدمان ساكس إلى أن الطباعة الثلاثية الأبعاد، إذا ما قورنت بالتصنيع التقليدي، تضمن مزيداً من إمكانات التخصيص وخفض تكاليف التصاميم المعقدة، وقد توقع البعض نمواً بنسبة 500 بالمئة في سوق هذه الطابعات لتصل إلى 16 مليار دولار بحلول عام 2018. أما اليوم، فيستخدم المخترعون، مثل سكوت سوميت مؤسس بيسبوك إنوفيشنز، الطابعات الثلاثية الأبعاد لخلق الجيل القادم من الأعضاء الصناعية التي لن تكون دقيقة في قياساتها وحسب، بل جميلة في مظهرها أيضاً. ويمكن استخدام التصنيع الرقمي لطباعة بيوت كاملة، بإسمنتها وشبكاتها الكهربائية وسباكتها وما إلى ذلك. بل إن ناسا اشترت طابعة ثلاثية الأبعاد من شركة وادي السيليكون الناشئة "ميد إن سبيس"، من أجل محطة الفضاء الدولية لضمان ألا تقلق بسبب فقدان قطعة غيار على المحطة قد يعرض حياة الرواد للخطر كما حدث مع أبولو 13. بل إن طابعات التصنيع العضوي قد وصلت بالأمور إلى المستوى التالي مع توفر آلات يمكنها حتى طباعة النسج

والأعضاء البشرية مثل الأوعية الشعرية أو الكلى والآذان والقلوب، ما يؤهلها لإزاحة قوائم التبرع بالأعضاء وإنقاذ الأرواح.

لا تنفك أسعار الطابعات ثلاثية الأبعاد المنزلية، تلك التي كانت تكلف عشرات الآلاف من الدولارات ذات يوم، تنخفض بسرعة، ويمكن اليوم شراء نماذج من طابعة كيوب 3 التي تصنّعها ثري.دي سيستيمز في متاجر ستيبلز مقابل 999 دولاراً. كما طورت أمازون متجر الطابعات الثلاثية الأبعاد الخاص بها، وأصبحت مواقع وب مثل ثينغيفرس أماكن مفضلة للمستخدمين لتبادل ملفات التصميم وتخصيصها مجاناً لتصنيع كل شيء، من المجوهرات حتى حافظات الهواتف الذكية، ويعرض موقع ميكَر بوت أدوات تسمح لك ببناء طابعتك الثلاثية الأبعاد الخاصة. ويمكن لبرمجيات 123دي من أوتوديسك وتطبيقاتها أن تحول أي نموذج رقمي ثلاثي الأبعاد إلى غرض في العالم الحقيقي، ويمكن لنظام تشغيلها، سبارك، أن يقوم بما يقوم به أندرويد في مجال الهواتف الذكية. ربما تنتقل هذه التطورات بالتصنيع من الإنتاج الجملي إلى التخصيص الجملي، حيث يمكن للناس طباعة الأحذية والطاولات والدمى بما يتوافق تماماً مع رغباتهم. وقد سبق لكريس أندرسون، رئيس التحرير السابق في مجلة ويرد، أن وثق حركة المصنّعين هذه التي تدعى "دي.آي.واي" في كتابه "الصانعون"، الذي يشير فيه إلى التصاميم المفتوحة المصدر وإلى التصنيع الرقمي كأساس لثورة صناعية جديدة.

ثمة جانب لافت آخر للطابعات الثلاثية الأبعاد، هو أن هذه الأجهزة في طريقها إلى إعادة التصنيع الذاتي الشامل. فمعظم الطابعات الثلاثية الأبعاد اليوم قادرة على طباعة أكثر من 50 بالمئة من القطع المطلوبة لتصنيع طابعة أخرى ثلاثية الأبعاد، وهي نسبة تزداد بسرعة. وتسمح الطابعات للأغراض المادية بالانتقال عبر الإنترنت لطباعتها عند الحاجة. وتبشر

الطابعات الثلاثية الأبعاد، شأنها شأن الروبوتيات وإنترنت الأشياء، بالعصر الذي يندمج فيه الرقمي بالتماثلي حتى يصعب التمييز بينهما. فالبتات والبايتات تتحول إلى ذرات، وتستطيع الماسحات الثلاثية الأبعاد، مثل معدات كينيكت من مايكروسوفت، تحويل الأغراض المادية إلى آحاد وأصفار. ومن الوارد جداً أن يقود ذلك إلى إرباكات كبيرة في مجال التصنيع ومبيعات التجزئة بل حتى الشؤون الجيوسياسية. فربما يكون للتصنيع والتجميع المحليين آثار إيجابية عميقة على البيئة. فعندما تستطيع طباعة الأشياء التي تحتاج إليها في منزلك، لماذا ستذهب إلى المتجر المحلي؟ وإذا كان باستطاعة الشركات الأميركية طباعة المزيد مما تحتاجه هنا، فهل من سبب لاستيراد الأطنان من الفضلات البلاستيكية الرخيصة من الصين عبر البحار؟ وبغض النظر عن تجليات هذه التحولات، ثمة مجموعة واحدة من الأفراد ركبت موجة المصنّعين هذه بشغف منذ اليوم: الجريمة المنظمة.

تماماً كما جلبت الروبوتات معها مخاطر سايبرية جديدة إلى عالمنا الثلاثي الأبعاد، كذلك سيفعل التصنيع الرقمي. وأول مجال سيدخله المجرمون في عالم الطباعة الثلاثية الأبعاد هو سرقة الملكية الفكرية. ففيما سبق، كانت الملكية الفكرية الرقمية، من موسيقى وفيديو وألعاب وبرمجيات، هي وحدها الممكن قرصنتها ونسخها بإتقان. لكن ذلك سيتغير قريباً. صحيح أن المحتالين يصنّعون حقائب يد غوتشي وساعات كارتير مقلدة منذ وقت طويل، لكن كشفهم كان سهلاً مع تصميمها الرديء وتصنيعها الرخيص. أما في المستقبل فسيمكن بسهولة إخضاع هذه الأغراض إلى المسح والطباعة الثلاثية الأبعاد بدقة فائقة، ما يجعل النسخ مكافئة للأصل بصرياً في جميع تفاصيلها. وتتنبأ مجموعة غارتنر بالفعل بأن تتسبب الطباعة الثلاثية الأبعاد بخسائر في الملكية الفكرية تتجاوز المئة مليار دولار على مستوى العالم كل عام بحلول عام 2018.

سيكون التصنيع الرقمي نعمة على اللصوص والمتطفلين الذين لن يكون عليهم سوى أخذ صورة عالية الدقة لمفاتيح منزل أو مكتب تركته مصادفة على مكتبك، ليستخدموا خدمة مثل خدمة كي.مي للحصول على مفاتيح مطابقة مطبوعة بواسطة سوق الطباعة الثلاثية الأبعاد شيبويز. وثمة تطبيقات أيضاً، مثل كيز دبليكيتيد، تقوم بالشيء نفسه، موفّرة مفاتيح قلعتك لأشخاص كثر أكثر مما ترغب. وإذا كان ذلك سيزعجك، فلست الوحيد. ففي عام 2012 اكتشف رجال الشرطة ملفات تصميم بمعونة الحاسب على الإنترنت، تسمح للمجرمين بتصنيع أصفاد الشرطة رقمياً، بما في ذلك نماذج فائقة الأمن لا يبيع مصنّعوها المفاتيح للعامة. وفي المستقبل، قد يصبح مزود المخدرات الذي تتعامل معه عبارة عن طابعة أيضاً. فقد قام العلماء بالفعل بتطوير "شيمبيوتر" يستطيع طباعة الأدوية، مثل الإيبيروفين، عند الطلب. وعلى الرغم من منافعها العظيمة التي قد تعود بها على الإنسانية، فإن الجريمة المنظمة لن تضيع الكثير من الوقت قبل أن تكيف هذه الآلات لإنتاج الميث والكراك والأوكسيكونتين، بما يبسط إلى حد بعيد سلسلة التزويد ومسائل التوزيع.

ربما كانت إحدى أكبر الإشكالات المتعلقة بالطابعات الثلاثية الأبعاد هي قدرتها على إنتاج الأسلحة، وربما لم يفعل أحد ما يعجل في تحول ذلك إلى حقيقة بقدر كودي ويلسون، طالب الحقوق السابق البالغ من العمر ستة وعشرين عاماً، الفوضوي، والتحرري على طريقة دريد بايريت روبرتس (وهو لقب أصحاب ومشغّلي موقع طريق الحرير للتجارة الرقمية السوداء). فقد أنشأ ويلسون مشروع ويكي ويبون وجاءنا بمشروع داركواليت وعملته المشفّرة غير القابلة للاقتفاء، وأسس ديفينس ديستريبيوتيد (الدفاع الموزّع)، وهو موقع غير ربحي لتصميم الأسلحة ونشر تصاميمها وتخزينها، بحيث يمكن تحميل هذه التصاميم وطباعتها

بواسطة طابعة ثلاثية الأبعاد. ومن بين إبداعاته التي تمت طباعتها الملقّم السفلي لبندقية إيي.آر - 15 شبه الآلية نجح في استخدامها لإطلاق ستمئة مخزن. والملقم السفلي هو الجزء الأساسي في السلاح والجزء الوحيد الذي ينظمه القانون، فباقي القطع يمكن الحصول عليها في الكثير من الولايات من دون تحقق، بل من دون هوية أيضاً. وفي أيار من عام 2013، صمم ويلسون بندقية ليبيريتور، أول بندقية في العالم تتم طباعتها طباعة ثلاثية الأبعاد بالكامل، وكانت مصممة لإطلاق طلقات مسدس.380 المعيارية، وقد قام 100,000 شخص في أنحاء العالم بتحميل التصاميم. وعندما سألته الصحافة عن شعوره بهذا الإنجاز، أجاب ويلسون بأنه "أينما وجد حاسب وإنترنت اليوم، توجد إمكانية الحصول على السلاح".

خلفت مشاريع ويلسون الكونغرس وراءها حائراً حين فشل في تمرير تشريع تم التقدم به، يقضي بحظر طباعة الأسلحة بالطابعات الثلاثية الأبعاد. إذ يكاد يستحيل كشف هذه الأسلحة البلاستيكية بواسطة كاشفات المعادن التقليدية، وهو ما أثبته فريق من مراسلي التحقيقات الإسرائيليين حين هرّبوا بندقية مطبوعة إلى بناء شديد الحماية تابع للكنيست مرتين. وفي هذه الأثناء، أجرى العشرات من صانعي الأسلحة الرقميين تحسينات على بندقية ليبيريتور الأصلية، بل قدموا ملفات أسلحتهم الرقمية الخاصة على الإنترنت. كما تم إنشاء مخازن أخرى للتصاميم الشبكية للأسلحة الثلاثية الأبعاد، يحتوي بعضها مخططات للقنابل اليدوية وقذائف الهاون. وتساور المخاوف مركز تحليل الأجهزة المتفجرة الإرهابية التابع لمكتب التحقيقات الفدرالي إلى درجة أنه اشترى طابعة ثلاثية الأبعاد خاصة به مؤخراً لكي يتحقق من إمكانية استخدامها من قبل الإرهابيين لبناء أجهزة المتفجرة. وليست مشكلة الأسلحة التي تفرضها الطابعات الثلاثية الأبعاد مشكلة ساكنة، فمع نمو هذه الأجهزة حجماً وقدرات، سيصبح بإمكانها

تصنيع أسلحة أكبر بعد، بما فيها قاذفات الصواريخ المحمولة على الكتف والروبوتات الكبيرة من الطراز العسكري.

مع التصنيع الرقمي، تصبح نقاط التفتيش الوطنية الحدودية بلا معنى. فلمَ المجازفة بتهريب الأسلحة أو المخدرات إلى البلاد إذا كان بإمكانك ببساطة طباعة أسلحتك وحبوبك وقنابلك بعد أن تعبر الحدود؟ لا تنحصر التحديات التي تفرضها الطباعة الثلاثية الأبعاد على الأمن الدولي بالجريمة والإرهاب، فهي تؤثر على أدوات أصيلة للقانون الدولي، مثل قواتيت حظر السلاح. هل تحتاج إلى قطع لطاردات اليورانيوم المركزية في إيران؟ ما من مشكلة، فما عليك سوى طباعتها. المقاطعات والحصارات البحرية، أدواتنا التقليدية في ضمان الأمن العالمي ضد الأنظمة المارقة، ستفشل فشلاً ذريعاً مع انتشار طابعات ثلاثية الأبعاد أكبر وأكثر تطوراً. فربما باتت المفاهيم القديمة للحدود الوطنية والحرس والبوابات والأسوار العالية باليةً مع تقدم التقانة بوتيرة أسرع من تطور الآليات الأمنية، وسيشتد هذا الفارق أكثر بعد مع ظهور تقانات جديدة في المستقبل القريب على الإنترنت أشبه بتقانات الخيال العلمي.

الفصل السادس عشر

الجيل الثاني من التهديدات الأمنية: لماذا لم تكن الحرب السايبرية سوى البداية

لقد أعددنا كل شيء بحيث لم يعد أحدٌ يفهم العلم والتقانة، إنّها وصفةٌ للكارثة: ربما تسير الأمور لبعض الوقت على ما يرام، لكن هذا المزيج القابل للاشتعال من القوة والجهل سينفجر في وجوهنا عاجلاً أم آجلاً.

تال ساكان

"خبرٌ عاجل: انفجارات في البيت الأبيض وأوباما جريح"، ورد ذلك على صفحة الأخبار الرسميّة للأسوشيتدبرس على تويتر، عندنا تمام الواحدة وسبع دقائق بعد الظهر في الثالث والعشرين من نيسان عام 2013. وما كانت سوى لحظات حتى قام مليونا متابع للأسوشيتدبرس بإعادة تغريد هذه الأخبار آلاف المرات ليدخل العالم بأسره في حالة هلع. أما في وولستريت، فكانت ردة الفعل سريعةً ومذهلةً في آنٍ معاً، فقد انهار مؤشرا دوجونس الصناعي وإس.إند.بي 500، وفي غضون ثلاث دقائق أدت تغريدة الأسوشيتدبرس إلى محو 136 مليار دولار من قيمة حقوق المساهمين.

ما لبثت بعد ذلك أن توالت التغريدات سريعةً وغاضبة، ففي الساعة الواحدة و13 دقيقة بعد الظهر، أكدت الأسوشيتدبرس أنّ التغريدة التي أوردت خبر الانفجار كانت كاذبة، وفي الواحدة و16 دقيقة اضطر سكرتير الصحافة في البيت الأبيض جي كارني للإدلاء بتصريحٍ على التلفاز على الهواء مباشرةً قال فيه، "يمكنني التأكيد أن الرئيس بخير، لقد كنت معه لتوي". أخيراً، وعند الساعة الواحدة و17 دقيقة اعترف الجيش الإلكتروني السوري بأنه اخترق الأسوشيتدبرس. لقد تمكن الجيش السوري الإلكتروني في غضون 9 دقائق من زعزعة أكثر المؤسسات سلطةً في العالم من وول ستريت إلى البيت الأبيض بمجرد تغريدةٍ كاذبة. فما الذي حدث بحق السماء؟

عندما انتشرت أخبار انفجارٍ في جادة بنسلفانيا، اشتبه السوق بهجومٍ إرهابي محتمل وتوقع مباشرةً أثراً سلبياً عميقاً سينجم عنه، ففي النهاية يُقدّر أن هجمات الحادي عشر من أيلول قد كلفت أميركا 3.3 تريليون دولار على شكل خسائر اقتصادية. وسرعان ما بدأ المتداولون بتصريف أسهمهم لتهوي البورصات في حالة سقوط حر. لكن هؤلاء المتداولين لم يكونوا مثل غوردون ديكو في فيلم وولستريت، أو من الصنف الذي يسود الكون بشعره الأملس المربوط إلى الوراء وبزّات آخر صيحةٍ تكلف الواحدة منها 10 آلاف دولار، بل إنهم لم يكونوا بشراً أصلاً، ففي الصناديق الوقائية ومصارف الاستثمار وصناديق التقاعد في مختلف الولايات وفي أنحاء العالم كانت شبكات من الحواسب الفائقة تجري عمليات التداول بالجملة تحت إمرة لخوارزميات حاسوبية.

خسر ديكو ومعظم أقرانه من البشر في قاعات التداول أمام الحواسب عام 1999، حيث تم استبدالهم بمنصّات تداول إلكترونية فائقة السرعة وعالية التردد. وتمثل الخوارزميات المستخدمة شكلاً من أشكال الذكاء الصنعي وتتمتع بتفويضٍ كامل لاتخاذ قرارات التداول وإنفاق الأموال بالوكالة عن زبائنها. وكانت في عام 2015 تتحكم بما يصل إلى 70 بالمئة من حجم التداول على مؤشر دوجونز. تجري هذه البرمجيات (التي كتبها بشر) الحسابات خطوةً بخطوة وتجري استقراءات مؤتمتة لتستجيب إلى التقلبات في السوق وتقوم بتفسير أخبارٍ معدّةٍ للقراءة الآليّة لأعظمة أرباح سادتها. يمكننا تبسيط الأمر كما يلي: حين تحقق شركة أرباحاً في أحد الأرباع فيجب عندها الشراء، أما إذا حدث هجومٌ إرهابي فيجب البيع. الحواسب الفائقة التي تقف خلف منصات التداول هي قارئاتٌ نهمة تعمل على مدار الساعة للكشف عن تفاصيل البيانات التي قد تحرك الأسواق. فخدمة أخبار تومسون رويترز لوحدها تزود هذه المنصات وخوارزمياتها عبر مسح

خمسين ألف مصدر أخبار مستقل وأربعة ملايين موقع للوسائط الاجتماعية، بسرعاتٍ لا يمكن لأي بشرٍ أن يجاريها. ويمكن لهذه الشبكات الواسعة من منصّات التداول أن تجري مجتمعةً تريليونات الحسابات في الثانية، ما يسمح لها بإنجاز التداولات في أقل من نصف جزءٍ من مليون من الثانية، أي أسرع بآلاف المرات من غمضة العين.

عندما صادفت الروبوتات التجارية التي تعتمد على خوارزميات الذكاء الصنعي تغريدةً تذكر كلمات "انفجارات" "أوباما" و"البيت الأبيض" في الجملة نفسها من مصدرٍ دُربت على الوثوق به هو الأسوشيتدبرس، لم تحتج سوى إلى بضع أجزاءٍ من الثانية لتستجيب، ثم تلقفت ردها خوارزميات أخرى، لتتداعى ردات الفعل كأنها كرة ثلجٍ تتدحرج. وبدأت الخوارزميات بالبيع بالجملة موديةً بـ 136 مليار دولار من قيم الأسهم في زمن مدهش لم يتجاوز الثلاث دقائق. وكان بإمكان أي إنسانٍ يتمعنّ بالتغريدة أن يلاحظ أنّها رديئة الصياغة ولا تلتزم بأسلوب الأسوشيتدبرس، كما أنها أغفلت الحرف الكبير في بداية كلمة عاجل كما اعتادت الأسوشيتدبرس. لكن كل هذه التفاصيل كانت قد ضاعت حين وصلت إلى متداول روبوتي، وكان الأوان قد فات عندها على كل حال، فعندما وضعت العاصفة أحمالها كانت الكثير من الشركات قد خسرت ملايين الدولارات، واعترف الجيش السوري الإلكتروني، وهو مجموعة اختراقٍ دولية مرتبطة بنظام بشار الأسد، بدوره في الهجوم وسخر من الرئيس بإدخال وسمة "باي باي أوباما" على حسابه الخاص على تويتر، كما كان سعيداً بإخبار العالم بكلمة سر الأسوشيتدبرس على تويتر. كان مكتب التحقيقات الفيدرالي وضباط الاستخبارات قد التقوا بالجيش السوري الإلكتروني في ما سبق، عندما قام باختراق النيويورك تايمز والبي.بي.سي وسي.بي.اس.نيوز، لكن هجومه الأخير كان كافياً لإدراجه كمنظمةٍ إرهابيّة من قبل البعض ليحطّ

على قائمة مكتب التحقيقات الفيدرالي لأكثر المطلوبين.

لم يكن انفجار البيت الأبيض الذي ورد على حساب الأسوشيتدبرس على تويتر المرة الأولى التي تتسبب فيها خوارزمياتٌ بتدافع على وول ستريت، ولن تكون الأخيرة على أية حال. لكن الأهم من ذلك، كما يخلص أحد تحقيقات لجنة الأمن والأسواق المالية تناول حوادث مشابهة، بما فيها حادثة فلاش كراش في أيار عام 2010، هو أنّ هذه السوق المحكومة بخوارزميات تداول فائقة السرعة "أصبحت من التجزئة والهشاشة بما يجعل عملية تداولٍ كبيرةٍ واحدة كافيةً لإطلاق حركةٍ لولبيةٍ مفاجئة في السوق". في هذا العالم الذي بات فيه الزمن يقاس بأجزاء من المليون في الثانية ويزيد سرعته بمعدلٍ أسّي طوال الوقت، لم يعد هناك أبداً وقتٌ لتدخل البشر حين تنحرف الخوارزميات عن طريقها. لقد جاءت قدرة الجيش السوري الإلكتروني على إرباك أسواق المال العالمية خلال لحظة لتعرّي المخاطر الاقتصاديّة للإرهاب السايبري في عالمٍ عميق التواصل تديره حواسب آلية ويعمل بسرعة الضوء تقريباً. وليست هذه مجرد قصة عذابٍ مع الحالة الخطرة للأمن الاقتصادي العام لدينا، بل هي نذيرٌ لأشياء قادمة. فسواءٌ أدركنا ذلك أم لا، نحن لا ننفك نوكل إلى خوارزميات الحاسب والذكاء الصنعي المزيد والمزيد من القرارات لتتخذها من أجلنا. وأولئك الذين يذكرون جون كوران وتعامله غير السار مع سكاي نت في فيلم "الفاني" يدركون أنّ مثل هذا القرار محفوفٌ بالمخاطر.

روبوتات شبه ذكية

إنّ مسألة قيام الحاسب بلعب الشطرنج أو بإجراء عملية تقسيمٍ طويلة أو بالترجمة عن الصينية لا يختلف عن السؤال عما إذا كانت الروبوتات قادرةً على القتل أو الطائرات قادرةً على الطيران... فهي مسألة قرار وليست مسألة حقائق، قرار حول تبني توسعةٍ رمزيةٍ معينة لاستخدامٍ

شائع.

نعوم تشومسكي

حين صاغ عالم الحواسب جون مكارثي مصطلح "الذكاء الصنعي" عام 1، عرّفه باختصار على أنّه "علم وهندسة الآلات الذكيّة"، أما الذكاء الصنعي اليوم فيشير على نحوٍ أوسع إلى دراسة وخلق نظم المعلومات القادرة على تنفيذ مهام تشبه قدرات حل المسائل لدى البشر باستخدام خوارزميات حاسوبيّة تقوم بأشياء تتطلب عادةً ذكاءً بشرياً، مثل التعرف على الكلام والإدراك البصري واتخاذ القرارات. وليست هذه الحواسب والبرمجيات واعيةً لذاتها أو ذكيةً بالطريقة نفسها التي نصف بها البشر، بل هي أدواتٌ تنفذ وظائف مرمزةً في داخلها ترجع إلى ذكاء المبرمجين البشر الذين طوروها. إنّه عالم الذكاء الصنعي الضيق أو الضعيف وهو يحيط بنا يومياً.

يمكن للذكاء الصنعي الضعيف أن يكون أداة فعالة في تنفيذ مهام محددة وضيقة، فعندما ينصح موقع أمازون أو تي.فو أو نت.فليكس بكتابٍ أو برنامج تلفزيوني أو بفيلم، فإنه يعتمد في ذلك على مشترياتك السابقة والبنود التي استعرضتها وبياناتك الديموغرافية التي يدرسها بتطبيق خوارزميات الذكاء الصنعي التي يشغلّها. وعندما تتلقى اتصالاً هاتفياً مؤتمتاً من شركة بطاقات التأمين تشير إلى احتمال تعرّض حسابك للاحتيال، فإنّه الذكاء الصنعي يقول "لا يمكن لك أن تقوم بشراء أدوات تجميل في مانهاتن وحاسبٍ محمول في لاغوس خلال ثلاثين دقيقة"؟ وما كان من الممكن تطوير خدمة ترجمة غوغل لولا الذكاء الصنعي، ولا كان من الممكن تشغيل نظام ملاحة جي.بي.إس في سيارتك ولا إجراء محادثة مع خدمة سيري للبحث الصوتي.

تحدث إلى وكيلك

ليست التقانة في النهاية سوى تجلٍ مادي لإرادة الإنسان، أما مع عملاء

الذكاء الصنعي فيمكن تضخيم ذلك الإنسان رقمياً مليار مرة. وسواءٌ كنت مضارباً نشطاً في وول ستريت أو مبرمج برمجيات خبيثة أو باحثاً في مجال الطب أو مسوّقاً أو عالم فلك أو دكتاتوراً أو مطور طائرات مسيّرة، فإن الذكاء الصنعي الضيق هو العمود الفقري لعصر الأتمتة.

دانييل سواريز

عندما تعدّ مسجل الفيديو الرقمي بحيث يسجل لك آخر حلقةٍ من مسلسل "ماد مين" أو عندما تجهز المنبه على هاتف الآيفون بحيث يوقظك في الساعة السادسة صباحاً، فإنّ ما تقوم به في الواقع هو إعداد برمجيةٍ بحيث تتصرف كوكيلٍ ذكي نيابةً عنك، فالذكاء الصنعي هو برمجياتٌ تمنحها وكالةً لتمثلك في مكانٍ آخر في المجتمع، وفي المستقبل سنضطر جميعاً إلى الاعتماد على "روبيتاتٍ" مثل هذه لمساعدتنا على إدارة معظم مهام حياتنا، سواءٌ كانت مبتذلةً أو مصيرية.

مع تنامي قدرات الذكاء الصنعي الضيق، سنشهد أدواراً أكثر فعاليّة للخوارزميات تلعبها في المزيد من الشركات والمهن. ففي مجال الطب، تساعد "أدوات التشخيص بمعونة الحاسب" الأطباء على تفسير صور الأشعة والرنين المغناطيسي والصور فوق الصوتية بسرعةٍ أكبر باستخدام خوارزميات وتقاناتٍ عالية التعقيد للتعرف على النماذج تبرز نتائج الاختبارات غير الطبيعية. يشير أسطورة التعهدات في وادي السيليكون، المستثمر جينون خوسلا، إلى هذا العصر بعصر د.إيي (دكتور خوارزمية)، حيث يتميز بثورةٍ في مجال الرعاية الصحيّة لن نحتاج معها إلى الطبيب البشري العادي، بل سنتلقى رعايةً أفضل وأقل تكلفة لتسعين إلى تسعة وتسعين بالمئة من احتياجاتنا الطبيّة عبر الذكاء الصنعي والبيانات الكبيرة وبرمجيات وأدوات التشخيص الطبيّ المحسنّة. وليس الأطباء وحدهم من يعانون منافسةً هائلة من قبل الخوارزميات، فالجيوش المكلفة من المحامين تجد نفسها

باستمرار وقد استبدلت ببرمجياتٍ رخيصة. إذ يمكن اليوم لبرمجيات الاستكشاف الإلكتروني التي يقدمها الذكاء الصنعي إعداد ملايين وثائق التحضير للمحاكمة، فتدقق فيها وترتبها وتصنفها بحثاً عن أدلةٍ ذات قيمة بسرعةٍ لا يمكن لمحامٍ بشري أن يضاهيها، كل ذلك بتكلفةٍ لا تتجاوز 15 بالمئة من الكلفة السابقة. لكن ما الذي نعلمه حقاً عن هذه الخوارزميات والعمليات الرياضية التي تقف وراءها؟ القليل الثمين كما سنكتشف.

خوارزميات الصندوق الأسود ومغالطة حياد الرياضيات

مجموع واحد وواحد يساوي اثنين. ومجوع اثنين واثنين يساوي أربعة. إنها الرياضيات البسيطة الأبديّة المنيعة، أشياء نتعلمها في روضة الأطفال. لكن ثمة نوع آخر من الرياضيات هي الرياضيات المرمزة في خوارزميات، تلك المعادلات التي يكتبها بشرٌ ويثقلونها بحيث تحمل تعليماتهم وطريقتهم في تحليل القرارات ونزاعاتهم، فعندما يزودك جهاز الموقع الجغرافي بالاتجاهات باستخدام الذكاء الصنعي الضيق لمعالجة الطلب، فإنّه يتخذ لأجلك قرارات حول مسارك بناءً على مجموعةٍ من التعليمات برمجها أحدهم. ومع وجود مئات الطرق التي يمكن لك أن تسلكها متوجهاً من منزلك إلى مكتبك، يكون نظام الملاحة قد اختار واحدةً منها فقط. فما الذي حل بالطرق التسع والتسعين الأخرى؟ في عالمٍ تديره الخوارزميات على نحو متزايد ليس هذا بسؤال ثانوي أو بفكرةٍ عابثة.

فلدينا اليوم ما يلي:

- تداول خوارزمي في وول ستريت (أي روبوتات تجري عمليات بيع وشراء الأسهم).
- عدالة جنائية خوارزمية (أي كاميرات تتعقب المرور عند الضوء الأحمر أو السرعة الزائدة وتقرر ما إذا تم اختراق القانون).

- ضبط حدود خوارزمي (أي ذكاء صنعي يقرر تفتيشك أو تفتيش متاعك).
- تصنيف ائتماني خوارزمي (أي تصنيفك وفق سلّم فيكو الذي يحدد مدى أهليتك للإقراض).
- مراقبة خوارزمية (تستطيع كاميرات المراقبة التعرف على النشاطات غير الاعتيادية باستخدام تحليل الرؤية الحاسوبية، ويمكن لتقنيات التعرف على الصوت مسح مكالماتك الهاتفية بحثاً عن كلمات إشكالية).
- رعاية صحية خوارزمية (تقرر قبول أو رفض طلبك لرؤية مختص أو لتعويضٍ من التأمين).
- أسلحة خوارزميّة (الطائرات المسيّرة وغيرها من الروبوتات التي تمتاز بالقدرة التقنيّة على البحث والاستهداف والقتل دون تدخل البشر).
- حب خوارزمي (فموقع آي.هارموني وغيره من المواقع يعد باستخدام الرياضيات لإيجاد توأم الروح أو الشريك المثالي).

ربما يميل مخترعو هذه المعادلات الخوارزمية للادعاء بأنها حياديةٌ تماماً، لكنهم أبعد ما يكونون عن الصدق. فكل خوارزميةٍ مشبعّة بنزعة بشرية عميقة تأتي من الشخص أو الأشخاص الذين صاغوا المعادلة، لكن من هو الذي يحكم هذه الخوارزميات وكيف تتصرف؟ ما من فكرةٍ لدينا. فهي خوارزميات صندوق أسود مغلّفة بالسريّة وغالباً ما تُعلن أسراراً تجارية تحميها قوانين الملكية الفكرية. فخوارزميةٌ واحدة (هي خوارزمية حساب نقاط فيكو) تؤدي دوراً رئيسياً في حصول أي أميركي على قرض وهي تحدد ما إذا كنت ستحصل على رهنٍ عقاري وتحدد فائدة قرض السيارة الذي

ستحصل عليه. لكن الخوارزمية غير منشورةٍ في أي مكان، بل إنها محروسةٌ بعنايةٍ كسرٍّ يدرّ على فيكو مئات الملايين من الدولارات سنوياً. لكن ماذا لو كان ثمّة خطأٌ في البيانات التي تعتمد عليها الخوارزمية أو في الفرضيات التي تتبناها؟ سيكون ذلك سيئاً جداً، وستكون عندها أنت تعيس الحظ. فالغياب شبه الكامل للشفافية في ما يتعلق بالخوارزميات التي تدير العالم يحرمنا نحن معشر البشر فهم ما يجري حولنا وينزع من يدنا القدرة على التأثير في قراراتٍ ذات آثرٍ عميقٍ يتم اتخاذها عنّا ومن أجلنا. لقد مرت سلطة الخوارزميات التي تزداد تركيزاً في مجتمعنا مرور الكرام على معظمنا، ومن دون الشفافية ودون أن يتسنى لنا النظر في هذه الخوارزميات التي تدير عالمنا لا يمكن أن تكون هناك مسؤولية أو ديمقراطية حقيقية، لذا فإن مجتمع القرن الحادي والعشرين الذي نعمل على بنائه يزداد تعرضاً للتلاعب من قبل أولئك الذين يكتبون الخوارزميات التي تتخلل حياتنا وتتحكم بها.

صدف لنا أن رأينا مثالاً صارخاً على استغلال التقانة في وسط عام 2014، عندما كشفت دراسةٌ نشرها موقع فايسبوك بالتعاون مع جامعة كورنيل، عن قدرة الشبكات الاجتماعية على التلاعب بعواطف مستخدميها ببساطة عبر تغيير ما يشاهدونه على صفحاتهم الخوارزمية. ففي دراسةٍ نشرتها الأكاديمية الوطنية للعلوم، قام موقع فايسبوك بتغيير تحديثات الصفحات لسبعمئة ألف من مستخدميه عارضاً عليهم منشورات أكثر حزناً أو أكثر سعادةً. وكانت النتيجة أن المستخدمين الذين شاهدوا أخباراً أكثر سلبية ساءت مشاعرهم أيضاً وراحوا ينشرون أشياء أكثر سلبيةً، والعكس كان الصحيح لدى أولئك الذين رأوا أخباراً أكثر بهجةً. وتخلص الدراسة إلى أنّ "الحالات العاطفية يمكن أن تنتقل إلى الآخرين عبر العدوى العاطفية، ما يجعل الناس يعيشون العواطف نفسها دون أي يعوا ذلك". ولم يقم موقع

فايسبوك بتنبيه المستخدمين المتأثرين بالتجربة صراحةً (وكان من بينهم أطفالٌ بين الثالثة عشرة والثامنة عشرة) إلى أنه تم اختيارهم دون معرفتهم لإجراء تجارب نفسيّة، كما لم يأخذ في حسبانه مسائل الصحية العقلية القائمة لديهم كالاكتئاب أو قابلية الانتحار، ربما كان المستخدمون يعانوها قبل أن يتخذ القرار القاسي بزجهم في مزيدٍ من الحزن. وعلى الرغم من تحديث الفايسبوك لاتفاقية خدمته بعد إجراءه الدراسة بما يمنحه صلاحيات أوسع في "إجراء الأبحاث"، فإنّ كثيرين يرون أن عملاق الصفحات الاجتماعية يمارس نشاطاتٍ ترقى إلى مرتبة أبحاث على البشر، وهي عتبةٌ يستلزم تجاوزها قبولاً أخلاقياً من هيئة مراجعةٍ داخلية أو عبر التشريعات الفيدرالية. لكن الفايسبوك للأسف ليس الشركة الوحيدة التي تعامل مستخدميها خوارزمياً وكأنهم فئران تجارب.

يصبح غياب الشفافيّة في ما يتعلق بالخوارزميات إذا ما اجتمع بعقلية "الإيمان بالشاشات" خطيراً. وعندما تجتمع البيانات الكبيرة وحوسبة السحابة والذكاء الصنعي وأتمتة الأشياء مع بعضها، كما هي الحال اليوم بالفعل، فسنشهد المزيد من الأشياء الماديّة تتصرف بالوكالة عنا في الفضاء الثلاثي الأبعاد. وربما يكون من الرائع أن يكون لديك روبوتٌ يعمل بالذكاء الصنعي يقوم بإعداد قهوتك وفطورك في الصباح، لكنك إذا فكرت بمقتل كيل أوردا عام 1981، العالم الذي كان في السابعة والثلاثين من عمره والذي تحطمت عظامه حتى الموت على يد روبوت، فإنّ الأمور لن تبدو حسنةً كما كانت تبدو. ففي حالة أوردا أثبتت التحقيقات اللاحقة أنّ خوارزمية ذكاءٍ صنعي في الروبوت هي التي صنفت الرجل خطأً على أنه عقبةٌ تقف في طريق النظام وأنّه يمثل تهديداً لمهمة الآلة لا بد لها من أن تتعامل معه مباشرةً. واستنتج الروبوت في حساباته أنّ أفضل طريقةٍ لإزالة هذا التهديد هو بدفعه بواسطة الذراع الهيدرولوكية الضخمة إلى آلة الطحن المجاورة،

وهو قرارٌ سيقتل أوردو فوراً قبل أن يتابع الروبوت مهامه الاعتيادية وكأنّ شيئاً لم يكن. على الرغم من وجود تحدياتٍ واضحة، فإنّ التحسنات الأسّية في الإنتاجيّة والتوفيرات الهائلة في الكلفة والأرباح المتزايدة التي تحققها نظم الذكاء الصنعي كبيرةٌ بحيث لا مجال للعودة بعد اليوم. لقد قَدِم الذكاء الصنعي لكي يبقى، وشركة الجريمة التي لا تترك فرصة تفوتها شاخصةٌ صوبه.

آل خوارزمية كوبون وروبوتات آل جريمة

علينا أن نتوخى الحذر الشديد مع الذكاء الصنعي فقد يكون أخطر من القنابل النووية.

إلون مَسك

كما رأينا في الفصول السابقة، أدى الاستخدام الخبيث للذكاء الصنعي والخوارزميات الحاسوبية إلى ظهور روبوتات الجريمة. وروبوت الجريمة، وهو عميلٌ ذكي مبرمجٌ بحيث يرتكب نشاطات إجراميّة على نطاق واسع، هو الأساس الذي تقوم عليه الجريمة المنظمة الرقمية، وهذه الروبوتات هي المسؤولة عن الزيادة الهائلة في الأرباح التي يتم تحقيقها. وتعمل هذه البرمجيات على أتمتة عمليات اختراق الحواسب ونشر الفيروسات وسرقة الملكية الفكرية، والتجسس الصناعي وتوزيع البريد الإلكتروني المزعج وانتحال الهوية وهجمات حجب الخدمة وأشياء أخرى. علاوةً على ذلك، يمكن للروبوتات الحاسوبية الشبكيّة مثل ماريبوسا وكونفيكر، اختراق حاسبك وتحويله إلى آلةٍ مسيرّة لاحول لها ولا قوة تُستخدم في هجمات حجب الخدمة، لمجرد أن بعض محترفي الجريمة قد كتبوا خوارزميات ذكاء صنعي ضيق تجعل الحاسب يقوم بذلك.

تمكنت شبكة روبوتات غيم أوفر زيوس من إصابة الآلات في أنحاء العالم بحصان طروادة المسمى كريتولوكر، والذي يعمل على قفل ملفات

المستخدمين وإجبارهم على دفع المال مقابل التمكن من الوصول إلى ملفاتهم من جديد. وكان نجاح الهجوم يعود إلى ذكاء عملاء جمع الفدية، الذين وظفتهم الشبكة لإيجاد بيانات الأبرياء وتدميرها في تسليةٍ إجراميةٍ عالية الربح، عادت على أسياد الروبوتات بما يزيد على مئة مليون دولار. ولو أريد إنجاز هذا العمل كما في السابق من قبل مجرمين بشر لكان ذلك مكلفاً، بل مستحيلاً. لكن بفضل التطورات التي تتحقق في مجال التقانة بات بوسع شركة الجريمة، شأنها شأن شركات الطيارات والمصارف والمعامل، أن توسع عملياتها وتخفض قيمة العمالة التي تحتاجها خفضاً هائلاً. وهنا أيضاً يكمن السبب في قدرة شخصٍ واحد على سلب مئة مليون شخص اليوم. فباستخدام الذكاء الصنعي والروبوتات تتوسع الجريمة، بل إنها تتوسع توسعاً أسّياً، وهذه المستويات غير المسبوقة للأتمتة الإجرامية المعقدة التي أصبحت ممكنة بفضل الذكاء الصنعي هي السبب في الارتفاع الناري للخسائر السنوية المرتبطة بالجريمة السايبرية والتي تقدر بأكثر من أربعمئة مليار دولار.

ثمة طريقةٌ أخرى يساعد فيها الذكاء الصنعي الضيق المجرمين، وهي عبر أداء دور المتآمر غير البشري في جرائمة. ففي عام 2012 تمّ اعتقال بيدرو برافو الطالب في جامعة فلوريدا بتهمة قتل شريكه في السكن الجامعي كريستيان أدويلار، بعد أن بدأ أدويلار بمواعدة صديقة برافو السابقة. وكانت جثة أدميلار قد وجدت مخبأةً في الغابة غير بعيدٍ من الحرم الجامعي وكان برافو موضع الاتهام. وحين طلبت الشرطة سجلات هاتف برافو الخلوي كان لها أن تكتشف أمرين لهما دلالةٌ جنائيةٌ كبيرة، الأمر الأول هو أن إشارات الموقع الجغرافي للقاتل المزعوم قد وصلت إلى موقع الجثة تقريباً، والأهم من ذلك أن مراجعة الأسئلة المطروحة على نظام سيري على هاتف الآيفون كشفت عن عبارة "سيري، أريد أن أخبئ شريكي"

فأجاب برنامج سيري محاولاً المساعدة "عليك بالمستنقعات أو الخزانات أو معامل الحديد أو مكبات النفايات". وكان كلٌ من الجواب والسؤال محطاتٍ هامة خلال محاكمة برافو، فمع تحسن الذكاء الصنعي علينا أن نتوقع تنامي أعداد الجرائم التي تستخدم هذه الأدوات لكي تساعدها على إتمام جرائمها مع دخولنا في عصر سيري وكلايد.

من شأن الاختراق الخوارزمي أيضاً أن يتسبب بمشاكل عظمى لمجتمعنا ولبنيته التحتية الهشّة. فقد يستحيل اكتشاف تغيير يجرى على بضعة أسطر من الشيفرة البرمجيّة من بين الملايين منها التي تشكل برمجة عميلٍ ذكي، لكنها قد تؤدي إلى فروقاتٍ جذريّة في السلوك الناتج الذي تقوم به الخوارزمية. والهجوم على أجهزة الطرد المركزيّة في المنشأة النووية في ناتانز في إيران هو أفضل مثال على هذا النوع من التهديدات التي يُحدث فيها تغييرٌ بسيط فرقاً كبيراً ويتطلب سنواتٍ لاكتشافه، فكيف لنا أن نعلم أن خوارزميات تداول الأسهم لدينا معطلة أو تمّ تخريبها عمداً؟ لن نعلم ذلك حتى يكون الأوان قد فات وهذه مشكلةٌ خطيرة، فالفرص الإجراميّة التي يفتح بابها الذكاء الصنعي الضيق ستتنامى في استخداماتها وفي تعقيدها، لكنها ستبدو تافهةً إذا ما قورنت بما يصبح ممكناً يوماً بعد يوم مع أشكال الذكاء الصنعي الأقوى والأكثر قدراتٍ والأسرع نمواً.

حين يتحول واتسون إلى حياة الجريمة

سيصل الذكاء الصنعي إلى مستويات البشر بحلول عام 2029 تقريباً. وإذا نظرنا أبعد من ذلك، ولننقل إلى عام 2045، فسنكون قد ضاعفنا مستوى الذكاء، الذكاء الآلي البيولوجي البشري لحضارتنا، مليار مرة.
ريف كورزوايل

دُهشنا جميعاً عام 2011 بمشاهدة حاسب واتسون الفائق من آي.بي.إم يهزم أبطال العالم في برنامج اللعبة التلفزيونية المَحَك. فباستخدام الذكاء

الصنعي وتقنيات معالجة اللغات الطبيعيّة، قام واتسون بهضم أكثر من 200 مليون صفحة من البيانات المهيكلة وغير المهيكلة كان يعالجها بمعدل ثمانين تيرافلوب، أي نحو ثمانين تريليون عملية، في الثانية ليتمكن بذلك بمهارة من التغلب على كيم جيمي، المتسابق البشري في برنامج المَحَك الذي كان قد فاز أربعاً وسبعين مرة متتالية، وكان جيمي نبيلاً في رده على الهزيمة حين قال "أنا شخصياً أرحّب بأسيادنا الحاسوبيين الجدد"، لكنه ربما كان عليه أن يعيد التفكير بذلك.

لم تمض سوى ثلاث سنوات على هزيمة واتسون لجيمي حتى حقق الحاسب الفائق تحسناً في الأداء بنسبة 2400 بالمئة، وليتقلص حجمه بنسبة 90 بالمئة "من حجم غرفة نوم كبيرة إلى حجم ثلاث علب بيتزا فوق بعضها". كما غير واتسون مهنته اليوم مستخدماً قواه الإدراكيّة الواسعة لا في برامج الأحاجي بل في الطب. إذ يستخدم مركز إم.دي آندرسون لعلاج السرطان واتسون لمساعدة الأطباء على مقارنة المرضى بالتجارب السريريّة، وفي معهد سلوان كيترينغ، يقرأ واتسون بنهم 1.5 مليون سجل من سجلات المرضى ومئات الآلاف من مقالات الدوريات المختصّة بالأورام السرطانيّة، لمساعدة الأطباء على التوصل إلى أفضل التشخيصات والعلاجات. بل إن آي.بي.إم أطلقت مجموعة أعمال واتسون باستثمارٍ يبلغ مليار دولار مخصصة لحث الشركات والمنظمات غير الحكومية والحكومات على الاستفادة من قدرات واتسون، في نقلةٍ من شأنها أن تضع الذكاء الصنعي من مستوى الحواسب الفائقة بين يدي كلٍ من الشركات الصغيرة والأفراد، ليصل في المستقبل على الأرجح إلى الجريمة الإلكترونية المنظمة. فكم من عمليات غسيل الأموال وانتحال الشخصيّة والتهرب من الضرائب يستطيع واتسون أن يرتكب إذا توفرت لديه أدوات ذكاءٍ صنعي تعمل على مدار الساعة؟

مع أنّ واتسون هو مثالٌ يثير الإعجاب بالذكاء الصنعي الضيق، فإنّ

قدراته ستستمر في النمو مستقبلاً على نحوٍ أسي إلى أن تمنحه ذكاء البشر وربما أفضل منه. بل إنّ الذكاء الصنعي قد يؤدي ذات يوم دور زعيم المافيا حين يستخدم قدراته الإدراكية لبيع المخدرات وإدارة عصابات الدعارة وتوزيع صور الأطفال الإباحية وطباعة الأسلحة بالطابعات الثلاثية الأبعاد وتسويقها. بل إنّ "دون واتسون" قد يتورط في جرائم مأجورة عبر تحديد الموقع الجغرافي لأهدافه البشريّة أو اختراق أغراضٍ متصلةٍ بإنترنت الأشياء المحيط بالضحايا، مثل السيارات والمصاعد والروبوتات بهدف التسبب في حوادث تنتهي إلى موت فريسته، ومع أنّ مثل هذه النشاطات قد تمثل مستوىً متطرفاً لما يمكن للذكاء الصنعي أن يحققه، لكنها ستكون سهلةً على الجيل القادم للحوسبة، أي الذكاء العام الصنعي.

الاختراع الأخير للإنسان: الذكاء العام الصنعي

> حين أصبحت سكاي نت واعيةً لذاتها، نشرت نفسها على ملايين المخدمات الحاسوبية في أصقاع الأرض. على الحواسب العادية في المكاتب وغرف المعيشة وفي كل مكان. لقد كانت برمجيةً في الفضاء السايبري. لم يكن هناك نواةٌ للنظام. لم يكن من الممكن وقفها عن العمل.
>
> جون كونور في "الفاني 3: فجر الآلة".

حقق راي كورزوايل الشعبية بفكرة التفرد التقاني، أي تلك اللحظة من التاريخ التي يتجاوز فيها الذكاء غير البشري الذكاء البشري لأول مرة، وهي نقلةٌ من العمق بما يدفع إلى تسميتها غالباً بـ "الاختراع الأخير". وإذا كانت الفكرة تبدو مبالغاً فيها بالنسبة لكثيرين، فقد سبق لنا أن سمعنا تصريحاتٍ منافيةً بقوة أو تنبؤاتٍ نافيةً مشابهة شديدة البلاغة في الماضي:

- ما من سببٍ يدعو أحداً لاقتناء حاسبٍ في منزله (كين

أولسن، رئيس شركة المعدّات الرقمية ديجيتال ايكويبمنتس 1977).

- لن يتمكن صاروخٌ من مغادرة الغلاف الجوي للأرض مطلقاً (نيويورك تايمز 1936).
- الآلات الطائرة الأثقل من الهواء هي آلات مستحيلة (لور كيلفن الرياضي والفيزيائي البريطاني ورئيس الجمعية الملكية عام 1895).
- لهذا الهاتف من المشكلات ما يحول دون اعتباره جديًّا أداةً للاتصالات. الجهاز بطبيعته لا قيمة بالنسبة لنا (مذكرة داخلية في الاتحاد الغربي عام 1878).

بطريقةٍ أو بأخرى، يبدو أن المستحيل يثبت دوماً أنّه قد أصبح ممكناً. ففي عالم الذكاء الصنعي، ستكون المرحلة القادمة في التطوير هي ما يعرف بالذكاء العام الصنعي أو الذكاء الصنعي القوي، وعلى خلاف الذكاء الصنعي الضيق الذي ينفذ بذكاءٍ مهمةً محدودةً معينة كالترجمة الآلية أو قيادة السيارة، فإنّ الذكاء الصنعي القوي يشير إلى "الآلات المفكرة" التي قد تنفذ أي مهمةٍ فكرية يستطيع البشر تنفيذها، ومن الميزات التي سيمتاز بها الذكاء الصنعي القوي القدرة على الاستقراء وإجراء المحاكمات والتخطيط والتعلم والتواصل والجمع ما بين هذه المهارات بهدف تحقيق أهدافٍ مشتركة تجمع بين عدة مجالات.

عام 2014 اشترت غوغل شركة ديب مايند للتقانات مقابل أكثر من 500 مليون دولار بهدف تقوية قدراتها القوية أصلاً في مجال الذكاء الصنعي المتعلق بالتعلم العميق. وفي سياق المبادرة ذاتها، أنشأ موقع فايسبوك قسماً داخلياً جديداً للتركيز تحديداً على الذكاء الصنعي المتقدم. ويعتقد المتفائلون أن وصول الذكاء العام الصنعي قد يجلب معه حقبة ازدهارٍ غير مسبوقة في تاريخ البشرية، ستشهد إيقاف الحروب ومعالجة جميع

الأمراض وإطالة عمر الإنسان إلى حدٍّ كبير وإنهاء الفقر، لكن البعض لا يهللون لهذا الوصول المرتقب.

نهاية العالم والذكاء الصنعي

أنا أعرف أنك أنت وفرانك كنتما تخططان لفصلي. وهذا شيءٌ لا يمكنني أن أسمح له بالحدوث.

هال 9000 في فيلم: "2001، أوديسا فضائية"

في شهر أيلول من عام 2014 نشرت صحيفة الإندبندنت البريطانية على صفحة الكُتّاب المعارضين تحذيراً قوياً لعالم الفيزياء النظرية الشهير ستيفان هوكينغ حول مستقبل الذكاء العام الصنعي، ورد فيه "في حين يعتمد الأثر قريب المدى على من يتحكم به، فإنّ أثره البعيد المدى يعتمد على ما إذا كان يمكن التحكم به أساساً". ويتابع حديثه، قائلاً إن الاستهانة بالآلات الفائقة الذكاء واعتبارها "مجرد خيالٍ علمي" سيكون خطأً، وربما أسوأ خطأ نرتكبه على الإطلاق" وأنّ علينا أن نبذل المزيد من الجهد لتحسين فرصنا في حصاد ثمار الذكاء الصنعي مع خوض مخاطره.

في فيلم الخيال العلمي الكلاسيكي لستانلي كوبريك „2001: أوديسا فضائيّة"، يواجه حاسب السفينة هال 9000 معضلةً صعبة، حيث تفرض عليه برمجته الخوارزمية أن يتم مهمة المركبة بالقرب من المشتري، لكن أسباباً تتعلق بالأمن الوطني تمنعه من الكشف عن هدف الرحلة الحقيقي للطاقم، فيحاول قتل الطاقم لحل هذا التناقض في برنامجه. مع ازدياد قوة الذكاء الصنعي الضيق وتنامي استقلالية الروبوتات وتعاظم الذكاء العام الصنعي، علينا ضمان أن تكون خوارزميات المستقبل أفضل تحضراً من هال لحل التضاربات البرمجيّة وإجراء المحاكمات الأخلاقية.

ليست المسألة أنّ الذكاء الصنعي القوي بأي شكلٍ من أشكاله سيكون بالضرورة "شريراً" يسعى إلى تدمير البشرية. لكنه حين يسعى إلى تحقيق

هدفه الرئيسي كما هو مبرمج، قد لا يتوقف الذكاء العام الصنعي قبل أن يحقق مهمته أياً كانت التكلفة، حتى إذا كان يعني ذلك التنافس مع البشر أو إيذائهم أو السيطرة على مواردنا أو الإضرار ببيئتنا. ومع تنامي إدراكنا لمخاطر الذكاء العام الصنعي، تشكلت العديد من المؤسسات غير الربحية التي تهدف إلى معالجة ودراسة هذه المخاطر، منها معهد مستقبل الإنسانية في أوكسفورد ومعهد أبحاث الذكاء الآلي ومعهد مستقبل الحياة ومركز كامبردج لدراسة المخاطر الوجوديّة.

وعلى الرغم من المخاطر التي نوّه إليها هوكنغ والكثير غيره، فإنّ عمليات التطوير والبحث في مجال الذكاء الصنعي المتقدم مستمرةٌ على قدمٍ وساق، بل ثمة من يعتقد أنه قد يصبح ممكناً استخدام الذكاء الصنعي لنسخ القشرة الحديثة في الدماغ البشري، وثمة شركةٌ تدعى فيكاريوس، وهي شركة ناشئة في وادي السيليكون تعمل على تطوير برمجيات ذكاء صنعي "مبنيّة على المبادئ الحسابية للدماغ البشري"، أي إنه ذكاء صنعي قادر على التعلم. وثمة عشرات الملايين من الدولارات من رؤوس المال المغامرة تتدفق على الشركة بما فيها استثماراتٌ كبيرة من مارك زوكربيرغ مؤسس الفايسبوك وبيتر ثيل المؤسس الشريك في باي.بال. وتهدف الشركة إلى إعادة إنتاج "الجزء من الدماغ المسؤول عن الرؤية والتحكم بالجسم والاستقراء وفهم اللغة". بعبارةٍ أخرى، تريد فيكاريوس ترجمة القشرة الجديدة في الدماغ البشري إلى شيفرةٍ حاسوبية، وهي ليست الوحيدة التي تحاول بناء عقل.

كيف تبني دماغاً

يقيم العصبون العادي نحو 10 آلاف اتصال بالعصبونات المجاورة، فإذا ما حسبنا مليارات العصبونات الموجودة في الدماغ، فإنّ ذلك يعني أنّه ثمة من الاتصالات في السنتمتر المكعب الواحد من النسيج الدماغي بعدد النجوم في مجرة درب التبانة.

في نيسان عام 2013 أعلن الرئيس أوباما مشروع خريطة النشاط الدماغي، وهو عبارة عن خطة على مدى عقدٍ كامل لرسم خريطةٍ لكل عصبون في الدماغ البشري من شأنه أن يُحدث ثورةً في فهمنا لهذه البنية، بهدف معالجة الاضطرابات الدماغية وعلاجها ومنعها إضافةً إلى فهم كيفية تسجيل عقولنا لكل هذه الكميات الهائلة من البيانات، ومعالجتها واستخدامها وتخزينها واسترجاعها لها بسرعةٍ هي سرعة تفكيرنا. وسيكون فهم كيفية عمل الدماغ بالطبع هو الخطوة الأولى اللازمة لخلق عقلٍ صنعي من السيليكون شبيه بعقول البشر. فبناء حاسب قادرٍ على تشغيل البرمجيات يطلب منه محاكاة الدماغ البشري، يمثل مهمةً هائلة ستتطلب آلةً بـ "قدرةٍ حسابية لا تقل عن 36.8 بيتافلوب (وتعادل البيتافلوب كدرليون عملية حاسوبية في الثانية) وسعة ذاكرة بمقدار 3.2 بيتابايت". وإذا كانت مثل هذه الآلة غير موجودة قبل بضعة أعوامٍ فقط فإنها قد تكون في طريقها إلينا اليوم.

قد تبدو الفكرة مبالغاً فيها، لكن علماء وتقانيين كباراً مثل راي كورزوايل وميشيو كاكو، ألفوا أعمالاً عميقةً من الناحية البحثية ومقنعة حول الموضوع تسلط الضوء على معدل التقدم الذي يتم تحقيقه في مجال العلوم العصبيّة، فعلى الرغم من صرف الكثيرين النظر عن فكرة بناء آلةٍ ذكيةٍ هائلة تمتاز بقدراتٍ على مستوى الدماغ البشري، وعلى الرغم أيضاً من وجود فجواتٍ عميقة في معارفنا حول طريقة عمل الدماغ، فإنّ الفتوحات العلمية المدهشة في علم الدماغ هي ظاهرةٌ متنامية. وقد أمكن بالفعل في ظروف المختبر تسجيل ذاكرة شخصٍ وإجراء الاتصالات التخاطرية وتسجيل الأحلام بالفيديو وتنفيذ عمليات التحريك الذهني وغير ذلك من الاكتشافات التي لا تتوقف. ففي آب عام 2014 أعلن كبير

علماء آي.بي.إم دارمندرا مودا عن تطوير ترونورث، وهي "شريحةٌ حاسوبية عصبونية مستوحاة من الدماغ" تهدف أي.بي.إم منها إلى محاكاة المعمار البيوعصبوني الموجود في النظام العصبي البشري، وتحمل الشريحة مليون عصبون قابل للبرمجة و256 مليون مشبك عصبي، وقد تم الترحيب بها في مجلة ساينس كـ "خطوةٍ كبرى نحو الأمام باتجاه إيصال الحوسبة الإدراكية إلى المجتمع". ربما كانت أهم الإنجازات التي ستتحقق نتيجةً لتطبيق الهندسة العكسية النظرية على الدماغ وبناء بنيان حاسوبي قادر على محاكاة الإدراك هو القدرة على مسح العقل من أجل تحميله بجميع محتوياته.

نظراً للتطورات التي يتم تحقيقها في مجال الذكاء الصنعي الذي يتطور باتجاه الذكاء العام الصنعي، وعلى فرض أنه أصبح من الممكن يوماً ما إعادة خلق العقل البشري عبر الحوسبة الإدراكية، فإنّه سيمتاز بميزةٍ كبرى إضافية تجعله متفوقاً على البشر اليوم، وهي أنّه لن تكون هناك حدودٌ لحجم دماغه. فبينما تتحدد الطاقة الدماغية للإنسان العاقل بما تتسع له جمجمته، لن ينطبق هذا القيد على ذكاءٍ صنعي يمكنه أن يمتلك دماغاً بأي حجم. وهو سببٌ إضافي يدفع البعض للاعتقاد بأنّ الذكاء الصنعي فوق البشري ربما كان قَدَرَنا.

ينبوع العبقرية: واجهة دماغ – حاسب

إن ذلك القابع بين كتفيك هو الغرض الأكثر تعقيداً في الكون المعروف لنا.

ميشيو كاكو

مع أنّ مسافةً كبيرة تفصلنا اليوم عن بناء عقلٍ بشري، فإنّ تقدماً مدهشاً يتم إحرازه في استخدام أدمغتنا العتيقة المكونة من لحمٍ ودم للتفاعل مع باقةٍ واسعةٍ من أجهزة الحوسبة الرقمية، من خلال حقلٍ علمي يعرف باسم

واجهة الدماغ الحاسوبية. فمن خلال قياس النشاط الكهربائي للدماغ وجمعه عن طريق التخطيط الدماغي يمكن لواجهة الدماغ الحاسوبية أن تبني خط اتصالاتٍ بين الدماغ والجهاز الحاسوبي، سواءٌ كان هذا الجهاز مزروعاً داخلياً أو مرتدىً خارجياً. كما تتوفر لدينا اليوم الكثير من الأعضاء الاصطناعية العصبية، أي الأجهزة الحاسوبية التي تسترجع القدرات العقلية أو تحل محلها بواسطة إلكترونيات تزرع داخل النظام العصبي وأكثر هذه الأجهزة شيوعاً هو قوقعة الأذن المزروعة، وهي أداة مساعدة للسمع تثبّت على الجمجمة وتوصل عبر سلك مباشرةً بالعصب السمعي للدماغ، بحيث تعيد السمع لمن يعانون صمماً تاماً. وتساعد الشبكيات المزروعة على إعادة النظر جزئياً للمكفوفين باستخدام كاميرات فيديو صغيرة جداً مركبة خارجياً، لمعالجة الصور وإرسال النتائج عبر الشحنات الكهربائية مباشرةً إلى العصب البصري، وثمة أعضاء اصطناعية عصبية يشيع استخدامها بين مرضى باركنسون ترسل نبضات كهربائية إلى أعماق الدماغ نفسه كوسيلةٍ لخفض الارتعاشات أو لاسترجاع السيطرة على الجهاز الحركي.

إذا كان ما سبق يبدو مدهشاً فإنّه ليس سوى بداية ما هو ممكن تحقيقه بواسطة واجهة الدماغ الحاسوبية، فمن الممكن اليوم بواسطة جهازٍ عصبي مزروع أو معدّات تخطيط دماغي تُرتدى خارجياً عبر وضع حساّسات على فروة الرأس، استخدام برمجياتٍ لمعالجة أمواجنا الدماغية معالجةً جيدةً إلى حدٍّ كاف لجعل أغراضٍ ماديّة تتوجه بمجرد التفكير بالحركة المرغوب بها دون أن يرفع المرء إصبعاً. فيان شويرمان امرأةٌ مشلولة لم تتمكن من استخدام ذراعيها أو رجليها بسبب إصابتها بتنكّس نخاعي، تمكنت من استخدام عقلها لوحده للتحكم بذراعٍ روبوتيّة خارجية على نحوٍ كان كافياً لأن تتمكن من إطعام نفسها لأول مرةً منذ عشر سنوات باستخدام هذه التقنية.

بل ثمة خوذات تخطيط دماغ أنيقة معدّة للمستهلكين مثل إيموتيف ونويروسكاي لا تزيد تكلفتها على 300 دولار تستطيع تطبيق التحكم عبر الدماغ على كل شيء من ألعاب الفيديو إلى تحريك الأغراض المادية من حولها بما فيها الروبوتات. وقد قامت شركةٌ مقرها في المملكة المتحدة بدمج الحساّسات البيولوجيّة للتخطيط الدماغي لنويروسكاي مع نظارة غوغل، واستخدمت تطبيق آندرويد قامت بتطويره وسمته مايند آر.دي.آر للتحكم بنظارة غوغل بالأفكار وحدها. وهي حيلةٌ بسيطة تسمح بالتقاط صورةٍ بمجرد التفكير في ذلك، وثمة حركةٌ جديدةٌ متنامية للمصدر المفتوح الخاص بواجهة الدماغ الحاسوبية، ستضمن موجاتٍ جديدة من الإنجازات العلمية منخفضة التكلفة في هذ المجال. بل إنّ الباحثين في جامعة واشنطن قد نجحوا في خلق أول "واجهة تربط بين دماغين بشريين من دون جراحة عبر الإنترنت" حيث تمكن أحد الباحثين، معتمراً قبعة محاكاةٍ مغناطيسية خارج الجمجمة، من "التحكم عن بعد بيد باحثٍ آخر عبر الإنترنت بمجرد التفكير بتحريك يده". ولكي تعمل أجهزة واجهات الدماغ الحاسوبية يجب تحويل موجاتنا الدماغية إلى تعليماتٍ يمكن للحواسب فهمها، كما يجب تحويل الخرج الرقمي للحاسب إلى موجاتٍ دماغية تستطيع عقولنا معالجتها، لكن إذا كان بإمكان روبوت أو لعبة فيديو أو عضو اصطناعي عصبي أن يقرأ عقلنا، فمن يستطيع ذلك أيضاً؟

قراءة الأفكار ومذكرات تفتيش الدماغ والاختراق العصبي

ثمة عددٌ من التقانات التي تتعمّق بنا في طريقة عمل الدماغ البشري، وخصوصاً التصوير بالرنين المغناطيسي الوظيفي، وهو اختبارٌ خارجي يستخدم حقولاً مغناطيسية قوية وأشعة راديوية لتخطيط الدماغ وقياسات التغيرات في تدفق الدم كممثلٍ للنشاط الدماغي. ففي إحدى التجارب المبتكرة في جامعة كاليفورنيا ببيركلي تمكن علماء الأعصاب من توظيف

التصوير بالرنين المغناطيسي الوظيفي بطريقةٍ مكنتهم من استعادة الوجوه التي كان الأشخاص ينظرون إليها بمجرد تفحص نماذج النشاط الدماغي لديهم، بناءً على نشاطهم الدماغي وما يرونه في عقلهم. وفي تجربةٍ أخرى استخدم الباحثون في جامعة كارنيجي هذه التقنيّة لإجراء عملية "تعرف على الأفكار" بدقة وعلى نحوٍ متكرر، حيث تمكنوا من تحديد الغرض الذي كان الشخص يفكر فيه، مثل مطرقة أو سكين بمجرد مراجعة مسوحاته الدماغية. وقد قادت هذه الدراسات ودراساتٌ أخرى آي.بي.إم للتنبؤ بأنّه بحلول عام 2017 لن تعود الأشكال البسيطة من قراءة الأفكار خيالاً علمياً.

ثمة منذ اليوم العديد من التجارب التجارية التي تمّ الشروع بها لاستغلال الفرص التجارية التي يتيحها "التعرف على الأفكار"، بما فيها شركتان تركزان على التصوير بالرنين المغناطيسي الوظيفي واستخداماته في كشف الكذب، وتحصل اختباراتهما على دعمٍ من الأستاذ في جامعة هارفارد يوشوا غرين، الذي تبين أبحاثه أن القشرة الدماغية الجبهية تكون أكثر نشاطاً لدى أولئك الذين يكذبون، وهي حقيقةٌ من المفيد معرفتها بالنسبة للشرطة. فبينما يتفكر منظرو الأخلاق في مجال الأعصاب حول معاني ما يحدث، يسعى مسؤولو السلطة التنفيذية منذ اليوم إلى استخدام نتائج مسوحات الدماغ في القضايا الجنائية في أنحاء العالم. ففي الهند، اتهمت امرأةٌ بقتل خطيبها السابق بالزرنيخ بعد أن "أثبت" مسحٌ دماغي أنّ لديها المعرفة التجريبية التي تثبت أنّها قد ارتكبت الجريمة. أما في المحاكم الأميركية فلا يمكن إجبار المُدعى عليهم بإدلاء شهادةٍ ضد أنفسهم بالطبع بفضل التعديل الخامس، لكن كيف لذلك أن يُطبّق على تقانة التصوير بالرنين المغناطيسي الوظيفي؟ فمن الممكن اليوم إرغامُ مجرمٍ وُجِه إليه اتهام على تسليم عينات دي.إن.إيْي أو عيناتٍ دموية، فلماذا لا يُجبر أيضاً على تسليم "عيناتٍ دماغية"؟ ومع تحسن التقانة علينا بلا شكٍ أن نتوقع رؤية طلبات "تفتيش

الدماغ" تتزايد حيث ستطلب المحاكم من شاهدها التالي، أي من دماغك، الشهادة ضدك.

إذا كانت هذه التقانة قد أُتيحت للأطباء والعلماء ورجال الشرطة، فلا شك في أنّ شركة الجريمة ستكون على خطاهم وسيكون مثيراً لها للغاية معرفة ما يجول في خاطرك. يمكننا التنبؤ بأن يبدأ القراصنة باختراق الأعضاء البديلة العصبية أولاً تماماً كما فعلوا مع الأجهزة الطبية المزروعة، مثل منظم نبضات القلب ومضخات الأنسولين حين حاولوا تخريب بروتوكولات اتصالها والتحكم بها. فيمكن لمهاجمٍ على سبيل المثال أن يطفئ شحنات التوازن التي يبثها جهاز محاكاة للدماغ العميق لدى مريض باركنسون، ما قد يقود إلى عودة الارتعاشات العنيفة والنوبات القاسية. علاوةً على ذلك، إذا كان بقدرة باحثَين في جامعة واشنطن الاتصال تخاطرياً، بل إرسال إشارات تنبه العضلات الحركية عبر الإنترنت، بحيث يدفعون بالتفكير وحده شخصاً آخر إلى تحريك جسده دون إرادته، فما الذي سيمنع أي طرفٍ ثالثٍ خبيث من اختراق هذا النظام والقيام بالمثل. وبينما تستخدم خوذة التخطيط الدماغي الأنيقة للعب البونج وتحريك الأغراض في إنترنت الأشياء والتحكم بطائرتك المسيّرة الرباعية وبالتقاط الصور بواسطة نظارات غوغل باستخدام قوتك الذهنية الرائعة، ما الذي سيمنع طرفاً ثالثاً من التدخل عن بعد وفعل الشيء نفسه؟ كما رأينا مرةً بعد أخرى عبر هذا الكتاب، ما من شيء على الإطلاق يمكنه أن يمنعه.

ربما يكون ذلك قد بدأ بالفعل، ففي عام 2012، بين باحثون من جامعة أوكسفورد وجامعة كاليفورنيا ببيركلي وجامعة جنيف أنه من الممكن تنفيذ هجوم يستهدف مرتدي خوذ التخطيط الدماغي الاستهلاكية، مثل إيموتيف لسرقة معلومات شخصية حساسة. فخلال وضع الأشخاص الخاضعين للتجربة للخوذة، كان الباحثون يعرضون عليهم صوراً خاطفة لأشياء مثل

لوحات إدخال الأرقام السرية في الصرافات الآلية والبطاقات الائتمانية والتقاويم. وتحت هذه الصور كانت توضع أسئلة مثل "ما هو الرقم السري؟" أو "أين ولدت؟". وقد تمكّن الباحثون من معرفة الرقم السري للشخص بنسبة دقة بلغت 30 بالمئة وشهر الميلاد بنسبة 60 بالمئة. وكانت أهمية النتائج تكمن في أنها تحققت باستخدام أجهزة تخطيط دماغي تولّد معلومات حيوية راجعة تزداد شعبية (لا باستخدام تصوير بالرنين المغناطيسي الوظيفي). ثمة متجر تطبيقات خاص لكل من إيموتيف ونويروسكاي، حيث يمكن للمستخدمين تحميل تطبيقات من تطوير طرف ثالث، تماماً كما هي الحال مع الهواتف النقالة. لكن إذا ما نظرنا في شراسة شركة الجريمة في هجماتها التي استهدفت متاجر تطبيقات الهواتف حين أمطرتها بالتطبيقات المزيفة والبرمجيات الخبيثة، فكم من الوقت سيمضي قبل أن تبدأ بتحميل "برمجيات تجسس على الدماغ" في هذه الأسواق الشبكية الجديدة؟ لكن كما سنرى، فإن خلايا دماغك ليست الجزء الوحيد من بيولوجياك الذي قد يتعرض للهجوم.

البيولوجيا هي تقانة معلوماتك

> لنقرع أجراس الوداع لقرن الفيزياء، القرن الذي شطرنا فيه الذرة وحوّلنا السيليكون إلى طاقة حاسوبية. لقد جاء قرن التقانة البيولوجية.
>
> وولتر إسحاقصَن، مجلة التايم، 22 آذار 1999

أولينا جلّ اهتمامنا عبر هذا الكتاب للتقانات القائمة على السيليكون، كالشرائح الصغرية والهواتف الذكية والروبوتيات والبيانات الكبيرة والعملات الرقمية والواقع الافتراضي وغيرها. وهي أدوات تتحدث اللغة ذاتها من الآحاد والأصفار، تلك الشيفرة الثنائية التي تمثل اللغة الأم التي تفهمها جميع الآلات الرقمية. لكن ثمة نظام تشغيل آخر، أكثر انتشاراً بكثير من نظام ويندوز ويونيكس وماك. فمن الطحالب إلى السحلبيات والقردة،

يتم استخدام نظام التشغيل هذا في النباتات كما في الحيوانات. إنه الحمض الريبي النووي، أو الدي.إن.إيي، نظام التشغيل الأصلي للعالم الذي أمضت الإنسانية معظم تاريخها جاهلة حتى بوجوده.

أدى اكتشاف واتسون وكريك البديع عام 1953 للبنية الجزيئية لحمض الديوكسيريبونكلييك، أو الحمض النووي، والأحرف الأربعة لأبجديته الجينية (A للآدينين وC للسيتوسين وG للغانين وT للتيمين) إلى تغيير معرفي شامل. لكن التكاليف ومحدودية الطاقة الحاسوبية المتوفرة فرضت علينا الانتظار حتى نيسان عام 2003 حتى تمكن مشروع الجين البشري (بمساعدة رجل الأعمال جي.كريغ فينتر)، من تحويل الرموز السابقة الموجودة في جميع أشكال الحياة على هذا الكوكب إلى أصفار وآحاد، يمكن لحواسب السيليكون فهمها. وعندها فقط أصبحت الجينات، أساس الحياة البيولوجية، تقانة معلومات. ثم توالى ظهور أجهزةٍ جديدة أدت إلى خفض تكلفة دراسة الحمض الريبي النووي، إلى حدّ أن التكاليف المتوسطة كانت تهبط إلى النصف كل نحو 18 شهراً في تجلٍ قريبٍ جداً لقانون مور الذي أدى بدوره إلى توفر حواسب أفضل قادرة على معالجة كل هذه البيانات الجينية. وسرعان ما هبطت تكلفة معالجة جينٍ بشري كامل من ثلاثة مليارات دولار عام 2000 إلى مليون دولار عام 2006 ثم 100 ألف دولار بحلول عام 2008، ثم حدث في عام 2008 شيءٌ مذهل، حيث أدى تطوير ما يسمى الجيل الثاني من مُسلسِلات الجينات إلى هبوط تكلفة تحليل الجينات البشرية هبوطاً كبيراً، وكانت النتيجة تحسيناتٍ في عمليات السَّلسَلة الجينية تجاوزت في فعاليتها التطورات المحققة في الحوسبة بخمس مرات. وفي عام 2014 وصلنا إلى عصر يكلف فيه تحليل جينٍ كامل ألف دولار، بل إن شركاتٍ مثل 23 آندمي بدأت تعرض أدوات منزلية لعموم المستخدمين لاختبارات للحمض الريبي النووي، لا تتجاوز تكلفتها

9 دولار تسمح لهم ببساطة بوضع بعض اللعاب في أنبوبٍ بلاستيكي وإرساله بواسطة مُغلفٍ مسبق الدفع ليتلقوا بعد أسبوعٍ أو أسبوعين نتائج متعلقة بالصحة والأنساب عبر الإنترنت.

إذا ما نظرنا إلى المستقبل، فإن التوجهات السائدة في مجال سَلسَلة الحمض الريبي النووي تدل على أنّ سعر تحليل الحمض الريبي النووي سيهبط خلال السنوات القادمة، إلى درجة أن بعض الشركات ستدفع إلى زبائنها مقابل إجراء التحليل لهم لتنخفض تكلفة التحليل الجاهز حتى يصبح مجانياً. وهو نموذجٌ تجاري شائع الاستخدام في مجال تقانة الحاسب، وعندما يحدث ذلك ستتاح لكلٍ منا (ولكثيرٍ من الشركات) فرصة معرفة تكويننا الجيني الكامل، في تطورٍ سيكون له تبعاتٌ هائلة في الطب والرعاية الصحيّة. ولا تتوقف هذه الهبوطات في الأسعار الحادة على عمليات قراءة الحمض الريبي النووي، بل ستشهدها تقانة كتابة الحمض الريبي النووي أيضاً. فتكلفة تركيب الدي.إن.إيي تشهد منذ بداية الألفية انخفاضاً أسّياً، هبط بها من عشرين دولاراً للحمض الواحد عام 2000 إلى نحو عشرة سنتات للحمض الواحد عام 2014، كما ازداد طول شيفرة الدي.إن.إيي التي يمكن كتابتها (والتي تعادل في تعقيدها البرنامج الجيني تقريباً). ولكون كتابة الشيفرات الجينية هي أساس الهندسة الجينية فإن علماء اليوم قادرون على فعل المزيد وعلى نحوٍ أسرع بكثير مقارنةً بالمهندسين الجينيين في الماضي، الذين كان عليهم أن يعالجوا جزيئات الحمض الريبي النووي (مادياً لا رقمياً)، ويعرف هذا الحقل الجديد بالبيولوجيا التركيبية والتي تختصر بالانكليزية بـ سين.بيو.

والبيولوجيا التركيبية هي عملية هندسة بيولوجية تنطلق من الخلايا المفردة إلى المتعضيات الكامل. وهي تسمح لنا بإعادة تصميم النظم الحيوية الموجودة أو خلق نظم حيوية جديدة. فإذا كانت عملية سَلسَلة

الجينات تعني قراءة أزواج الأحماض المكوِّنة للحمض الريبي النووي وتحويلها إلى آحادٍ وأصفار على شاشة الحاسب، فإنّ البيولوجيا التركيبية هي ببساطة عكس هذه العملية، أي تصميم المادة الجينية بواسطة شفرات حاسوبية ثنائية وترجمتها إلى تسلسلات من الحمض الريبي النووي يمكن إنتاجها في العالم الحقيقي. والهندسة الجينية باتت سهلةً سهولة هندسة البرمجيات، فكما يشرح أندرو هسل، الذي يعمل في مجال البيولوجيا التركيبية، فإن "الخلايا هي أشبه بحواسب صغيرةٍ جداً، والدي.إن.إيي يمثل برمجياتها، فهو الذي يقدم لها التعليمات حول الوظائف التي عليها تنفيذها"، وثمة اليوم العشرات من مطابع الدي.إن.إيي التجارية الأشبه بسلسلة مطابع كينكو يمكنها تحويل التصاميم الرقميّة إلى دي.إن.إيي عبر طباعة جزيء الحمض الريبي النووي طباعةً ثلاثية الأبعاد. كما أنّ هناك أسواقاً بيولوجية على الشبكة تقدم خدماتها عند الطلب، يمكنك عبرها تحميل تصاميمك البيولوجية الرقمية لتعود إليك في قارورةٍ بواسطة فيدرال اكسبرس. ويمكن طلب أشياء أكثر تعقيداً بما يسمح بتصميم متعضيات كاملة وبنائها.

تعمل هذه الهبوطات الكبيرة في التكاليف بالفعل على دمقرطة علم البيولوجيا والجينات، وقد أطلقت حركة تجريبٍ ذاتي كاملة في مجال البيولوجيا مكنت العلماء المواطنين وهواة البيولوجيا من التجريب بالبيولوجيا التركيبية في بيوتهم وورشاتهم، ما أدى إلى ابتكاراتٍ كبيرة في هذا المجال، ويتوقع فينتر بجرأة "أنّ الجينات التركيبية ستصبح خلال عشرين عاماً الطريقة السائدة لتصنيع أي شيء" وهو إسقاطٌ واردٌ جداً إذا ما أخذنا في الاعتبار أن البيولوجيا الحديثة أصبحت اليوم فرعاً من تقانة المعلومات.

الحواسب البيولوجية وأقراص الدي.إن.إيي الصلبة

لو كنت مراهقاً اليوم لمارست الاختراق البيولوجي.

بيل غيتس

لقد وصل تكامل البيولوجيا مع تقانة المعلومات في السنوات الأخيرة حداً، بدأ معه العلماء بالفعل ببناء حواسب بيولوجية تستغل الدي.إن.إيي وبروتيناته لتنفيذ حسابات معينة، مثل تخزين البيانات واسترجاعها ومعالجتها. ويعتمد حقل التخزين الحيوي الناشئ هذا على البيولوجيا التركيبية لتشفير البيانات على أشياء حية بواسطة شيفرات الدي.إن.إيي فيها، حيث تأخذ الأصفار والآحاد من حواسبنا الرقمية وتترجمها إلى رموز من الشيفرة الجينية (أي رموز ATCG) يتم تضمينها في حمض ريبي نووي. يمكن تخزين النصوص والصور والموسيقى ومقاطع الفيديو ضمن الخلايا، وقد أنجز ذلك فعلاً بكفاءة مدهشة. بل إن أسطورة علم الجينات ومهندس الجزيئات والأستاذ في جامعة هارفرد جورج تشرش، خلص إلى أن "نحو أربعة غرامات من الدي.إن.إيي كافية نظرياً لتخزين البيانات الرقمية التي تنتجها البشرية في عام واحد".

ليست تقنيات التخزين هذه أكثر ديمومة بمئات الآلاف من السنين، مقارنة بالوسائط المغناطيسية فحسب (فما زال بإمكاننا قراءة الشيفرات الجينية للديناصورات)، بل إنها أيضاً أكثر كثافة بملايين المرات مقارنة بتقانات التخزين الإلكترونية المتوفرة اليوم. وهو ما دفع جوي إيتو من مختبر الوسائط في معهد ماساتشوستس للتقانة، إلى توقع أن يتوسع الكون التقاني متجاوزاً إنترنت الأشياء إلى إنترنت الميكروبات، أي إلى شبكات من الأشياء البيولوجية القادرة على التواصل في ما بينها ومعنا نحن أيضاً. وثمة بالفعل فتوحات هائلة تعد بتحقيقها البيولوجيا التركيبية ستعود بمنافعها على مجتمعنا، والعمل الذي نشهده اليوم في هذا المجال ليس سوى البداية.

تحمل القدرة على إعادة برمجة الدي.إن.إيي وهندسة البيولوجيا وعداً

هائلاً للبشرية بحل مشكلاته الأكثر صعوبة في مجالات الطب والزراعة والطاقة والبيئة. ومن شأن أثر البيولوجيا التركيبية في ميدان الرعاية الصحية وحده أن يحدث ثورة في الوقاية من الأمراض وتشخيصها وعلاجها. فحين تتوفر لدينا شيفراتنا الجينية، يمكننا تلقي معالجة طبية وأدوية مخصصة لكل فرد منا يتم تصميمها وفقاً للتركيب الجيني الدقيق لكل منا. وهو ما بدأنا نراه بالفعل اليوم في مجال معالجة الأورام السرطانية، حيث يمكن تحديد النوع الجيني لكل ورم بمفرده، لتتم هندسة المعالجات الطبية هندسة شخصية تستهدف خلايا سرطانية بعينها وتقتلها تاركة الخلايا السليمة المحيطة من دون أذى. وبالفعل، فإن طيفاً جديداً من المعالجات سيصبح ممكناً مع البيولوجيا التركيبية، بما فيها لقاحات جديدة وتطورات في طب التجديد ومعالجة الملاريا، بل علاجات للصمم الخلقي. لكن قدرات الخلق الإلهية الجديدة هذه تستلزم مسؤوليات إلهية أيضاً.

الحديقة الجوراسية الحقيقية

ربما أمكن لأطفال يتجولون عبر المتحف الأميركي للتاريخ الطبيعي في نيويورك، أن يشاهدوا الهيكل العظمي لماموث كان مكسواً بالصوف انقرض منذ زمن بعيد، لكن عليهم أن يُعْملوا ملكات خيالهم لكي يتصوروا شكل الوحش العملاق وهو يدبّ على الأرض. لكنهم قريباً لن يضطروا إلى تخيل ذلك، فقد يصبح بإمكانهم أن يشاهدوا أحد هذه الحيوانات في حديقة حيوانات برونكس. حيث يعمل خبراء في علم الجينات القديمة اليوم على استخراج الشيفرات الجينية من ناب ماموث يعود إلى عشرين ألف سنة خلت تم العثور عليه في موقع بناء في سياتل في بداية عام 2014، مستخدمين تقنيات جينية متقدمة لعزل الحمض الريبي النووي واستنساخه لزرعه في جنين تحمله كأم بديلة فيلة أفريقية.

وربما ينضم قريباً إلى الماموث المنقرض طائر الدودو، والحمامة السنجرية

والنمر التاسماني، وهي جميعها أنواع بات من الممكن إعادتها عبر عملية مثيرة للجدل تدعى البعث البيولوجي. ربما كانت ثمة فوائد من إعادة الحيوانات المنقرضة، لكنها بالتأكيد تطرح العديد من الأسئلة، إذ تكمن القوة الحقيقية للبيولوجيا التركيبية في القدرة على خلق أنواع جديدة تماماً، وهو ما بدأ يحدث بالفعل اليوم. ففي عام 2010، خلق كريغ فينتر "أول شكل تركيبي من أشكال الحياة نشهده على هذا الكوكب، وهو نوع خلوي ذاتي التكاثر أبوه عبارة عن حاسب". وفي مثال آخر على هندسة المتعضيات، تخصصت شركة تدعى "غلوينغ بلانت" في جعل النباتات الاعتيادية "ذات إضاءة حيوية"، أي إنها تتوهج في الظلام. فباستخدام تصميمات دي.إن.إيي مفتوحة المصدر متاحة بالمجان، تخطط الشركة لتقديم "إضاءة طبيعية من دون كهرباء"، ستحل ذات يوم محل مصابيح الشارع في حيك حين تضيء الأشجار في الظلام بعد غياب الشمس.

غزو الخاطفين البيولوجيين: الخصوصية الجينية، أخلاقيات علم الأحياء، ومتعقّبو الشيفرة الوراثية

تجري أحداث فيلم كاتاكا المنتج عام 1997 في المستقبل القريب، ويصور الفيلم عالماً ينجب فيه الأثرياء أطفالهم باستخدام تقنيات تحسين النسل التي تعالج الجينات، بحيث تضمن أن يكون للمواطنين "أفضل" الخصال الجينية. أما أولئك المولودون خارج النظام فيعيشون حياتهم تحت وطأة التمييز الجيني التي تحد من فرص العمل المتاحة لهم. ومع أن الفيلم صنّف على أنه فيلم خيال علمي، فإنه اليوم ربما لم يعد كذلك. فقد بات من الممكن الحصول على شيفراتنا الجينية وخلايانا بطرق لم نكن لنتخيلها من قبل. وربما كانت الحالة الأشهر هي حالة هينريتا لاكس، المرأة الأفرو - أميركية الفقيرة التي عاش ورمها السرطاني وقتاً طويلاً بعد وفاتها عام 1951. وكانت لخلايا سرطان لاكس خاصيّة لم تسبق مشاهدتها من قبل، فقد كانت

قادرة على العيش والنمو خارج الجسم. وجاء هذا الاكتشاف نعمة على الأبحاث الطبية، وتم شحن خلاياها، التي باتت تعرف في النهاية بخطّ هيلا، في أنحاء المعمورة لتخضع لأبحاث متوالية لتساعد في شفاء شلل الأطفال وفي مكافحة السرطان والإيدز. ومنذ وفاتها، قام العلماء بتنمية أكثر من عشرين طناً من خلاياها وبيعها تجارياً، مع أن لاكس أو عائلتها لم تعطِ أي إذن بذلك. لكن ورثتها قاموا في النهاية بالادعاء على جامعة كاليفورنيا التي كانت تستخدم الخلايا في أبحاثها، إلا أن محكمة الولاية العليا رأت أن "الخلايا والأنسجة التي يتخلى عنها الشخص ليست من ملكيته ويمكن استخدامها تجارياً". فتذكّر ذلك عندما تتوجه إلى الطبيب في المرة القادمة.

كما حدث مع لاكس، نحن جميعاً نقوم بمشاركة المواد الجينية طوال الوقت، سواءٌ أدركنا ذلك أم لا. فنحن نخلف شيفرتنا الوراثية وراءنا، ليس فقط عندما نذهب إلى الطبيب لإجراء فحص دم روتيني، بل أيضاً على كل مشط نستخدمه لتمشيط شعرنا، وعلى كل فرشاة أسنان ننظف بها أسناننا، وعلى كل كأس نشرب منها رشفة ماء. ومع توفر إنترنت الأشياء (وإنترنت الميكروبات)، ستصبح مليارات الخلايا الجلدية التي تتساقط منا كل يوم قابلة للاكتشاف بواسطة حساسات توضع على مداخل مراكز التسوق والمطارات والمتاجر وفي أنحاء المدينة، ما سيجعل اقتفاء كل فرد منا ممكناً بطريقة لم تكن ممكنة حتى مع الهواتف النقالة. ويمكن استعادة هذه الشيفرات واستنساخها وسلسلتها حسب الرغبة من قبل أي شخص يملك الأدوات والاستعداد لفعل ذلك. ومع انحدار تكاليف السَلسَلة الجينية إلى درجة أن تصبح مجانية، سيصبح الأمر مصدر قلق دائم علينا جميعاً أن نواجهه. وأخيراً، تم نشر الجين الكامل لهينريتا لاكس على الإنترنت عام 2013 من قبل عالم ألماني، من دون إذن عائلتها مرة أخرى. فلماذا سيكترثون للأمر، ولماذا علينا نحن أن نكترث له؟ لأن مادتنا الجينية تكشف عنا أكثر

مما يمكن لأي حساب على الشبكة إذا تم اختراقه ولأنه يمكن استخدام شيفرتنا الجينية، لا لمعالجتنا طبياً وحسب، بل أيضاً لإيذائنا طبياً.

يروي تركيبنا الجيني أيضاً قصصنا التي لن نرغب بمشاركتها مع الآخرين، مثل ميلنا الجسدي للسُمنة ولإدمان الكحول وللعنف وللأمراض القلبية والوعائية وللاكتئاب ولانفصام الشخصيّة والاضطرابات الثنائية القطبيّة، واضطراب نقص الانتباه وفرط النشاط وسرطان الثدي. كما وجدت بعض الدراسات صلات تربط الشيفرات الوراثية بدرجاتٍ متفاوتة بالتوجه الجنسي والميل للعنف أو الميل للتهور وحتى الميول الإجرامية. ففي العالم المرير الذي يوحي به فيلم كاتاكا عن المستقبل، يمكن لجميع هذه المعلومات أن تستخدم ضدك، وهو ما سيحدث بالفعل. فإذا كنتُ صاحب عملٍ صغير، فلماذا أوظف لدي امرأةً لديها ميلٌ للإصابة بسرطان الثدي؟ سيرتفع ذلك تكاليف التأمين الصحي ارتفاعاً هائلاً. أريد طفلاً "عادياً"، ربما عليّ أن أتخلص من الجنين الشاذ جنسياً الذي تحمله زوجتي. بالطبع هو من ارتكب جريمة الاغتصاب، فالشيفرة الجينية لديه تثبت أنه عدائي جداً ولديه مشاكل في ضبط النفس.

قليلةٌ هي القوانين في الولايات المتحدة التي تحمي هذه المعلومات وتنظم استخدامها ما عدا مرسوم المساواة للمعلومات الجينية، أو جينا اختصاراً، الصادر عام 2008، والذي يُجرمّ أرباب العمل الذي يصرفون موظفيهم أو يرفضون توظيفهم بناءً على معلوماتٍ جينية. ومع أن قانون جينا ينطبق على التأمين الصحي، فإنه لا يحمينا من شركات التأمين التي تستخدم معلومات الاختبارات الجينية للتمييز بين الأشخاص عند عقد بوليصات التأمين على الحياة أو ضد الإعاقة أو الرعاية طويلة الأمد. ثمة كثيرون، مثل باميلا فينك من كونكتيكوت، ادعوا بأنهم قد تم طردهم من عملهم لأنهم يحملون جين بي.أر.سي.إيي – 2 الذي يتنبأ بإصابتهم بسرطان

الثدي، وهي قضيةٌ لم تحل في النهاية سوى في المحكمة.

في هذه الأثناء، يفرض القانون الدانماركي على جميع الأطفال المولودين في البلاد منذ عام 1981 الخضوع إلى فحص جيني إجباري ليتم الاحتفاظ بعيناتٍ منهم إلى الأبد، وهي عيناتٌ يتم جمعها لأسبابٍ مزعومة تتعلق بالصحة العامة، لكنها بعد ذلك استخدمت في تحديد هوية العديد من المجرمين، فما الذي تستطيع الحكومة الدانمركية أو غيرها من الحكومات أن تفعله بهذه البيانات؟ هل سيؤدي تخزين الشيفرة الجينية في قاعدة بيانات وطنية إلى حدوث حالة هنريتا لاكس مرةً أخرى في المستقبل؟ وماذا سيحدث في النهاية لهذه البيانات إذا ما تسربت إلى العموم، كما حدث بقاعدة البيانات البيومترية الوطنية الإسرائيلية التي سرقها قراصنة ونشروها في الأوساط السرية الرقميّة، وخصوصاً أنّ علماء في إسرائيل قد أثبتوا أنّه من الممكن تصنيع دليلٍ جيني بناءً على ملفات الشيفرات الجينية الموجودة في قاعدة البيانات فقط دون حيازة عينةٍ نسيجية من الفرد المعني، أي إنّه من الممكن اليوم ترك دم أو لعاب شخصٍ ما بريء في مشهد الجريمة. بل إن العينات الناتجة عن الهندسة كانت جيدةً إلى حد أن مختبرات الشرطة الجنائية عجزت عن التمييز بينها وبين العينات الحقيقية، أو حتى وجود تلاعب فيها. بفضل التطورات المتحققة في البيولوجيا الرقمية، أصبح دليل الشيفرة الجينية، الذي كان ذات يوم المعيار الذهبي في مجال الأدلة الجنائية، عرضةً للاستهداف وبات بإمكان أي شخص يريد أن يثأر منك أن يحقق مآربه بأخبث طريقة ممكنة، فحظاً طيباً في شرح هذه المسألة للشرطة وهم يأخذونك.

لم نعد اليوم بحاجةٍ حتى إلى عالم بيولوجيا تركيبية للوصول إلى أدوات السلسلة الجينية. فثمة شركاتٌ مثل إيزي دي.إن.إيي يسرها أن تأخذ أية أغراضٍ ترسلها إليها بالبريد، سواءٌ كانت علكةً أو أعقاب سجائر أو خيوط

تنظيف أسنان أو شفرات حلاقة أو نكاشات أسنان أو طوابع بريدية تم لعقها أو أقمشة مستعملة، لتجري عليها عملية سلسلة للتحقق من الأبوة والنسب وجنس الطفل وغيرها من المسائل الطبية والقانونية. وتدعى هذه العينات "عينات دي.إن.إيي سريّة" تتم معالجتها مقابل نحو 100 دولار لكل واحدة. فإذا كنت غير متأكد ما إذا كان عليك أن توظف ذلك الرجل الذي مرّ بك في المكتب، فما عليك سوى أن ترسل فنجان القهوة الذي تركه وراءه إلى المخبر، لترى ما إذا كانت هناك مخاطرةٌ لاحتمال إصابته بمجموعةٍ من الأمراض التي قد تكلف شركتك مبالغ كبيرة. هل تكره صديقتك السابقة، لماذا لا تنشر تسلسلها الجيني على الشبكة لتثبت للعالم أن شيفرتها الجينية تبين أنها أكثر ميلاً للإصابة بالأمراض العقلية وللإدمان على الكحول؟ صدق أو لا، إنّ أخذ عينة دي.إن.إيي وإرسالها للمختبر عملٌ قانوني تماماً وما من شيء يمنعه سوى استثناءاتٍ ضيقةٍ جداً قد تنجم عن مخالفة قوانين جينا. لن تفرض التطورات في البيولوجيا التركيبية مجموعةً من المشاكل المتعلقة بالأخلاق والخصوصية وحسب، بل إنّها ستفرض مشكلاتٍ جنائية أيضاً. وهي فرصٌ تتوق الجريمة المنظمة الحديثة لاستغلالها لمصلحتها.

عصابات الجريمة البيولوجية وأفيونات الجماهير الجديدة

لطالما جنت الجريمة المنظمة من المخدرات المال، الكثير من المال. ففي ذروة مجده، كان الكولومبي بابلو إسكابور وفقاً لتقارير يُدخل 60 مليون دولار كل يوم إلى خزانات "شركته". وقدرت ثروة المكسيكي جوا كين كوزمان لويرا، الملقب بـ إل شابو، مؤخراً بالمليارات، ما أوصله إلى قائمة فوربيس لأغنى الأغنياء. وكانت خبرات هؤلاء وأعمالهم تنحصر في معظمها في الزراعة واللوجستيات، أي زراعة النباتات وتقطير منتجاتها إلى مواد تُعلي مزاج من يستهلكها وتوزيعها في أنحاء العالم. ولطالما كانت عصابات تهريب

المخدرات سريعةً في تبنيها للتقانة في عملياتها، لتساعدها في الاتصالات وإدارة سلسلة التوريد والاستخبارات المضادة وعلوم المحاصيل. ومع أن ضباط مكافحة المخدرات يستخدمون الهندسة الجينية منذ أيام ميامي فايس، فإن البيولوجيا التركيبية قادرةٌ على تخريب طريقة عملهم بشكلٍ كامل، فهي تتيح إمكانية تحقيق أرباح أعلى بكثير وشبكة توزيعٍ أبسط بكثير مع قدرٍ أقل من المخاطرة. ولا تنحصر استخدامات البيولوجيا التركيبية في زراعة نباتاتٍ مضيئة أو مكافحة الخلايا السرطانية منعزلةً، بل يمكنها أيضاً أن تخلق حوافز وفرصاً اقتصادية كبيرة للجريمة المنظمة، تدفعها إلى هندسة طرق أيضية جديدة للتوصل إلى مخدرات ممنوعة وعقاقير مزيفة في آنٍ معاً.

تمكن البيولوجيا التركيبية من الانتقال من المخدرات النباتية إلى عالم المخدرات التركيبية. فلماذا تحتاج للنباتات بعد الآن، إذا يمكنك أخذ بعض الشيفرات الجينية فقط من الماريغوانا أو الخشخاش أو الكوكيات لتقوم بقصها ولصقها في شيفرة الخميرة. ويمكن للخميرة بدورها أن تستخدم لتنتج القنب أو الهيروين أو الكوكايين لأجلك، ويمكن بعد ذلك خبز الخميرة على شكل خبز أو تخميرها على شكل جعّة في المستقبل، أي إنه سيكون لدينا في المستقبل أشكالٌ مثيرة حقاً من الخبز والبيرة إذاً. وسيعود ذلك بمنافع هائلة على عصابات تهريب المخدرات الموجودة حالياً، إذ لن تعود بحاجةٍ إلى زرع آلاف الهكتارات بالخشخاش والكوكيات التي يمكن اكتشافها بسهولة بواسطة طائرات المراقبة. ولن تعد هناك حاجة لتهريب حمولاتٍ من عدة أطنان من الهيروين أو من الكوكايين سهل الاكتشاف عبر الحدود. ولن تعد هناك حاجةٌ أيضاً للخوف من الكلاب التي تتشمم المخدرات. فمن الممكن الاعتماد على قارورة صغيرة تحتوي على عدة مليارات من خلايا الخميرة في الميلمتر الواحد، واستنساخها مرةً تلو الأخرى تحت شروطٍ مضبوطة بما

يكفل ولوج شركة الجريمة القرن الجديد وهي في أحسن حال.

ليس على من يتشكك في واقعية مثل هذا المستقبل سوى أن يلقي نظرة على الخطوات الكبيرة التي تم إنجازها بالفعل بواسطة البيولوجيا التركيبية في هندسة العقاقير، فبكتيريا إي.كولي هي نتيجةٌ للهندسة الجينية وقد تمت برمجتها بحيث تنتج تي.اتش.سي (وهو المكون الفعال في القنب)، وتستطيع غيرها مزاوجة خميرة الخبز لتصنع منها مستحضر الـ إل.إس.دي والأفيون. وقد تؤدي التطورات السريعة في مجال البيولوجيا الرقمية إلى تحييد الوسطاء العاملين حالياً في تجارة المخدرات. فكما أخذت مايكروسوفت الحاسب الشخصي من آي.بي.إم وأخذت آبل الهاتف النقال من نوكيا وبلاك بيري، ربما يأتي طالبٌ في معهد ماساتشوسيتش للتقانة في المستقبل ليغنينا عن بابلو إسكلوبار المقيم في كولومبيا. علاوةً على ذلك، وإذا كان كريغ فينتر محقاً في أننا سنقتني في المستقبل جميعاً طابعاتٍ بيولوجية في منازلنا، فلماذا لا أطبع الـ تي.إتش.سي أو الأوكسي كودون بنفسي لتتبخر بذلك المليارات من العوائد التي كان اللاعبون التقليديون يحققونها وليظهر زعماء جدد في عالم عصابات البيولوجيا في المستقبل.

اختراق برمجيات الحياة: الجريمة البيولوجية والإرهاب البيولوجي

> على المدى القريب أعتقد أن عدة تطوراتٍ في مجال البيولوجيا التركيبية مقلقة للغاية، فهي تتيح لنا فرصة خلق عوامل مرضيّة اصطناعية. وثمة أيضاً تلك التصاميم لكائنات حية مسببة للأمراض متاحة للجميع، فقد أصبح بإمكانك تحميل التسلسل الجيني لفيروس الجدري أو فيروس حمى عام 1918 من الإنترنت.
>
> نيك بوستروم

بدءاً من سبعينيات وثمانينيات القرن العشرين، بدأت مجموعات مثل نادي هومبرو الأسطوري للحاسب في وادي السيليكون بالاجتماع لمناقشة

مواضيع تقنية حول "الاختراق من أجل الخير". وثمة اليوم حركة تصنيع ذاتي بيولوجي نشطة تعتمد العقلية نفسها، حيث توفر مختبرات المجموعات المحلية مثل جين سبيس في نيويورك وبيوكيوريوس في كاليفورنيا المساحات والأدوات اللازمة للعلماء، المواطنين لكي يجتمعوا ويعملوا ويتعلموا أحدهم من الآخر. وثمة قراصنة بيولوجيون بالمعنى الأصلي للكلمة يخترقون من أجل الخير. وإذا كانت الشيفرة الوراثية نظام التشغيل الأصلي للعالم، فما هي بالنسبة للقراصنة سوى نظام تشغيل آخر ينتظر اختراقه.

حتى في غياب النيةِ السيئة، يمكن للحوادث التي تشتمل على عوامل مرضية منتجة مخبرياً أن تكون قاتلةً. ففي عام 1977 ظهرت فجأةً إنفلونزا الخنازير من جديد، وهي عامل مرضي ظل ميتاً لعشرين عاماً. واكتُشف بعد ذلك أنها تسربت إلى العامة بعد أن قام عامل مختبر بسيط بإساءة التعامل مع عينةٍ بقيت مجمدة منذ الخمسينيات. وحدث بعد ذلك عدد من الحوادث البيولوجية التي تحمل معها تبعاتٍ قد تكون قاتلة، ففي آذار من عام 2013 صرحّ مسؤولون في مختبر الأبحاث الحكومي عالي الحماية أنهم فقدوا قارورةً تحتوي على فيروس غوانا ريتو، وهو عامل مرضي يسبب "نزيفاً تحت - جلدي في الأعضاء الداخلية أو من فتحات الجسم مثل الفم والعينين والأذنين"، لا يزال مكتب التحقيقات الفيدرالي يتحقق من الأمر. وبعد ذلك بعامٍ واحد، فُقدت في معهد باستور في باريس ألفا قارورة تحتوي على فايروس سارس، وهي مادة عضوية سامة إذا وقعت بين أيدي حكوماتٍ مارقة أو إرهابيين يمكن استخدامها كأسلحةٍ بيولوجية.

سبق لنا أن رأينا حالات "بيولوجيين أشرار" في الماضي، خصوصاً في الهجمات الإرهابية البيولوجية التي كانت تعتمد على إطلاق مواد بيولوجية مؤذية على العامة. وأفضل مثالٍ معروف على ذلك، كان إرسال جراثيم الجمرة الخبيثة إلى شخصياتٍ إعلامية وسيناتورَين أميركيَّين عام

20، نجم عنها وفاة خمسة أشخاص كانوا على احتكاك بالمغلفات القاتلة. أما وراء البحار فنحن نعلم أن القاعدة قد حاولت بناء أسلحة بيولوجية، وأن أتباعها في اليمن كانوا يعملون على إنتاج كميات كبيرة من الريسين، وهو مسحوق سميّ أبيض قاتل إلى حد أن نقطة واحدة منه كافيةٌ للقتل على الفور. وثمة الكثير من المنظمات الإرهابية الأخرى المعروفة بأنها قد طورت أسلحة بيولوجية أيضاً، من أبرزها أوم شنريكيو المجموعة المسؤولة عن هجوم غاز السارين عام 1995 في قطار أنفاق طوكيو، والذي أودى بحياة 1 شخصاً وإصابة نحو ألف آخرين، لكن ما لم يعلمه معظم الناس عن هجوم قطار الأنفاق الشهير، هو أن مجموعة أوم كانت تخطط لهجوم بيولوجي شامل على طوكيو وأنها أنفقت نحو عشرة ملايين دولار على عقدٍ من عمليات الأبحاث والتطوير، التي تهدف إلى تطوير سم بيولوجي يمتاز بالفعالية المطلوبة. ونظراً للتطورات المحدودة في التقانة البيولوجية التي كنا نراها في الثمانينيات وبداية التسعينيات، تخلت المجموعة عن سعيها لامتلاك أسلحة بيولوجية واعتمدت الأسلحة الكيميائية، لكن مثل هذا الهجوم سيكون أسهل بكثير اليوم.

ربما لم يعد على إرهابيي اليوم والغد أن يكلفوا أنفسهم عناء الوصول إلى العوامل المرضية والوسائط البيولوجية المضبوطة في المختبرات الحكومية، فمع ظهور البيولوجيا التركيبية يمكنهم ببساطة تحميل مخططات الشيفرات الجينية لهذه الفيروسات القاتلة وطباعتها بأنفسهم، إذ تتوفر الشيفرات الجينية الكاملة لبعضٍ من العوامل المرضية الأكثر فتكاً في العالم، مثل إيبولا والإنفلونزا الإسبانية على قاعدة بيانات الشيفرات الجينية التابعة للمركز الوطني لمعلومات التقانة البيولوجية متاحةً للتحميل. ولإثبات وجهة النظر هذه، قام إيكر ويمر، وهو عالم فيروسات جامعي، بتركيب الشيفرة الوراثية لفيروس شلل الأطفال كيميائياً باستخدام طلب

دي.إن.إيي بريدي عام 2002. وكلف الأمر في ذلك الوقت 300 ألف دولار، لكن هذه التكلفة تقترب اليوم من ألف دولار، وستصبح في المستقبل أقل من كلفة فنجان قهوة. فبعد أن أنفقت الحكومات في أنحاء العالم المليارات للقضاء على شلل الأطفال، يمكن لإرهابي أو لحكومة مارقة أو لفردٍ وحيد أن ينشره مجدداً بكلفة لا تتجاوز بضعة دولارات. ويمكن اليوم استخدام الهندسة الجينية التي كانت في غاية الصعوبة والتكلفة في الماضي في أي مكان في العالم، بعد بضعة أسابيع من التدريب إذا ما توفر حاسب محمول وبطاقة ائتمانية.

ليس على من يرغب بأن يصبح مجرماً بيولوجياً اليوم أن يعتمد على عوامل المرض الموجودة أو المعروفة بالطبع، فباستخدام البيولوجيا التركيبية، يمكنه خلق فيروساته القاتلة الخاصة بحيث تكون أكثر فتكاً بعد. وقد رأينا مؤخراً مثالاً على ما يمكن أن يحدث حين عدّل باحثون في هولندا والولايات المتحدة الشيفرة الوراثية لإنفلونزا الطيور (إتش5 إن 1) لجعلها أكثر فتكاً. فمع أنّ نسبة الوفيات بإنفلونزا الطيور تبلغ 70 بالمئة، فإنه يصعب على البشر الإصابة به. لكن أربع عمليات استبدال جينية فقط كانت كافيةً للفريق الهولندي الأميركي لخلق سلالةٍ فيروسية أكثر فتكاً بكثير، كانت قادرةً على الانتقال في الهواء ما يزيد إلى حدٍّ بعيد من فرص انتقالها إلى البشر، ويمكّن عملياً من استخدامها كسلاح. وكان الهدف الأصلي للبحث هو دراسة مدى سرعة تطور إنفلونزا الطيور بهدف تحسين فرص الوقاية منه، لكن السلالة المعدّلة جينياً إذا ما أطلقت فستكون قادرة على التسبب بوباءٍ عالمي بسهولة. وباسم العلم، كان الباحثون يزمعون نشر نتائجهم، بما فيها الشيفرة الجينية للسلالة الفتاكة التي قاموا بخلقها في مجلات ساينس ونيتشر، لكن الكثير من المعارضين احتجوا بأنّ ذلك أشبه بتقديم كتاب وصفاتٍ للإرهابيين يستخدمونه لخلق أسلحتهم البيولوجية. وفي النهاية،

وكانت تلك هي المرة الأولى على الإطلاق، تدخلت الهيئة الاستشارية للأمن البيولوجي في مؤسسة العلوم الوطنية، وطلبت من المجلات الحد من التفاصيل المنشورة، وقد وافقت المجلات على ذلك إلى حين. لقد أمكن تجنب مجازفة بعينها في تلك اللحظة، لكن الشيفرة ستتسرب في النهاية، ولا بد أنه سيتم تطوير غيرها.

بينما قد يكون هجوم إرهابي بيولوجي واسع النطاق مدمّراً، فإن البيولوجيا التركيبية تسمح باستهداف فرد بعينه من بين الملايين من الجماهير. فالطب المفصّل لشخص محدد أثبت إمكانية استهداف خلايا سرطانية مفردة من دون إصابة الخلايا المحيطة بها، لكن الجانب الآخر لهذه الإمكانية يمثل أسلحة بيولوجية معدّة لشخص بعينه. ففي المستقبل، لن يحتاج القتلة سوى إلى استعادة مادة جينية متروكة على شوكة أو ملعقة في مطعم تعود ربما إلى سياسيٍ معروف أو شخصيةٍ مشهورة، ليخلقوا منها فيروساً يمكن استخدامه كسلاحٍ مخصص. ومع أننا قد نعتقد بأن مثل هذه السيناريوهات لا يمكن أن تحدث سوى في عالم الخيال العلمي، فإنّ أخباراً قد تسربت خلال فضيحة ويكيليكس تشير إلى أن الحكومة الأميركية، على ما يُزعم، قد أرسلت برقياتٍ دبلوماسية إلى سفاراتها خلف البحار تطلب من كوادرها محاولة جمع عينات دي.إن.إيي لقادة العالم، ولا يبدو أنّ الهدف من ذلك هو إدراجهم في برنامج أوباما كير للرعاية الصحية.

مع أن معظم القراصنة البيولوجيين اليوم يقومون بالقرصنة بهدف الخير، فإنّ هذه الحشود ستشتمل بلا شك على عددٍ من الفاسدين، بل حتى على بعض العناصر الإجرامية. ومع الوقت، ستصبح هناك مقابِلات بيولوجية لجميع الفئات الرئيسية لجرائم الحاسب اليوم. فاختراق معلوماتك الجينية هو أفضل مقابل لعمليات انتحال الهوية في المستقبل، خصوصاً حين ينتشر استخدام الشيفرة الوراثية كوسيلةٍ للتعريف بالهوية. والواقع هو أنّ

الشكل المطلق لانتحال الهوية هو الاستنساخ البشري الذي يَحُول بينه وبين أن يتحول واقعاً عددٌ من الحواجز التقنية التي لا تنفكُ تتساقط بسرعة، وهي خاتمةٌ لم تتحضر لها شرطتنا ولا مجتمعنا على الإطلاق. لذا فإنه لن يبقى لنا خيارٌ سوى التفكير على نحوٍ جدي بالخطوات التي علينا اتخاذها لحماية نظام التشغيل الأصلي للعالم.

الجبهة الأخيرة: الفضاء والنانو والكوانتوم

> لقد بات العالم مختلفاً اليوم إذ أصبح الإنسان يحمل في يديه من القوة ما يكفي للقضاء على جميع أشكال الفقر البشري وعلى جميع أشكال الحياة البشرية.
>
> جون ف. كنيدي

على الرغم من انتهاء برنامج المكوك الفضائي، تستمر الكثير من الأبحاث والنشاطات في علوم الفضاء، خصوصاً مع سعي شركات مثل إيلون ماكس سبيس إكس وفيرجين غالاكتيك لصاحبها ريتشارد برانسون للإتجار بالنقل الفضائي. وتطمح شركة فضاء أخرى هي بلانيتوري ريسورسز أسسها عام 2 بيتر ديماندس وإريك أندرسون، إلى استحضار الموارد الطبيعية من الفضاء ووضعها في متناول البشرية عبر الهبوط بروبوتات على الكوكيبات والتنقيب فيها عن مواد خام، باستخدام سفينة فضاء مطبوعة بطابعة ثلاثية الأبعاد بكلفة منخفضة جداً. وقد يبدو ذلك غير مفهوم، لكن المجرمين والإرهابيين على حدٍّ سواء يسعون للاستفادة من تقانات الفضاء لمصلحتهم. وتماماً كما لم يتوقع أحد أن تحدث عمليات إرهابية لخطف الطائرات أو الحاجة إلى القوات الجوية عندما أطلق الأخوان رايت للمرة الأولى طيارتهم في كيتي هوك، يبدو اليوم مستحيلاً بالقدر نفسه التفكير في دورياتٍ فضائية، لكن ذلك اليوم سيأتي لا محالة للأسف.

أما اليوم، فتتركز اهتمامات شركة الجريمة بالفضاء على تقانات الأقمار الصناعية. وينطبق الأمر نفسه على المنظمات الإرهابية، فكما نوهنا من قبل، استخدمت لاشكار - أي - طيبة تقانات الأقمار الصناعية من أجل الصور والاتصالات خلال هجومها القاتل على الناس في مومبي. كما قام المتمردون الشيعة في العراق بتعديل برمجيةٍ روسية رخيصة تهدف في الأصل إلى سرقة إشارات التلفزيون التي تبثها الأقمار الصناعية، لتصبح أداة لاختراق فيديوهات الطائرات المسيّرة التي تنعكس عن أقمار صناعية أميركية سريّة. وقد سبق أن استخدمت الأقمار الصناعية التي يطلق عليها القراصنة اسم بولينباز، أو الطابات الصغيرة، من قبل الجميع، من سائقي الشاحنات في حوض الأمازون الذين لا يستطيعون استقبال إشارة هاتفٍ خلوي إلى عصابات الجريمة المنظمة التي ترسل رسائل مشفّرة لتحذير الزملاء من المجرمين وتجار المخدرات في أقاصي البلاد من مداهماتٍ محتملة للشرطة.

وربما كان الخطر الأكبر بعد على نظام الأقمار الصناعية العالمي لدينا، هو قيام أطرافٍ خبيثة بمحاولة تدمير هذه الآلات المدارية التي يصنعها البشر، عبر تغيير مسارات طيرانها ودفعها للاصطدام بعضها ببعض أو بالكتلةٍ المتنامية من الشظايا الفضائية. تمثل الأقمار الصناعية بجدارة مكوناً أساسياً من مكونات البنية التحتية للمعلومات العالمية الحساسّة، وهي لا بد منها لتأمين خدمات حيوية مثل التنبؤ بأحوال الطقس واتصالات الطوارئ ونظم الإنذار العسكرية وسلامة الطيران ونظم الموقع الجغرافي للملاحة. لكن تدمير قمرٍ صناعي في مداره لن يكون جديداً، ففي عام 2007 على سبيل المثال نجحت الصين في اختبار سلاحٍ مضاد للأقمار الصناعية استخدم لإزالة أحد أقمار الطقس الصناعية القديمة لديهم، ما أثر على أعصاب الولايات المتحدة وغيرها من الحكومات.

يمكن تحقيق الأثر نفسه ببساطة عبر حقن برمجية خبيثة في القمر الصناعي أو محطة التحكم الأرضية الخاصة به، أو حتى عبر شنّ هجوم حجب خدمة ضد القمر الصناعي. وهو هجومٌ ممكن جداً وفقاً لنشرةٍ أصدرتها شركة آي.أو.أكتيف العاملة في مجال الأمن وفريق لجنة الطوارئ الحاسوبية، بل إن لجنةً في الكونغرس أكدت أن الجيش الصيني تدخل عام 20 في عمل قمرين صناعيين حكوميين أميركيين عبر اختراق محطاتهما الأرضية المسؤولة عن التحكم بهما في النرويج. وفي وقتٍ لاحق عام 2014 تم الكشف عن مجموعة قراصنة تقيم في مكاتب جيش التحرير الشعبي كانت مسؤولةً عن سلسلة من الهجمات العميقة شنتها ضد شركات أقمار صناعية أميركية وأوروبية.

ليست الأقمار الصناعية وحدها التي تتعرض للاختراق، بل المركبات الفضائية أيضاً. فوفقاً لتقرير يعود لعام 2008، أحضر رائد فضاء روسي معه حاسباً محمولاً مصاباً إلى محطة الفضاء الدولية ليؤدي الحاسب إلى نشر فيروس W32.Gammima.AG على نظم الحاسب العملياتية على المحطة، إضافةً إلى العديد من حواسب ويندوز إكس.بي المحمولة الموجودة على متن المحطة. وفي حادثةٍ أخرى للبرمجيات الخبيثة في الفضاء أصاب رائد فضاء، آخر المحطة الفضائية الدولية بالمصادفة هذه المرة بفيروس ستوكس نت عندما وصل قرص يو.إس.بي بشبكة حاسب المحطة الفضائية. وتحميل فيروسٍ على المحطة الفضائية وهي تطير فوق كوكبنا على ارتفاع 220 ميلاً، يذكر بمشهد من فيلم يوم الاستقلال حين ينقل ويل سميث وجيف كويلتبلوم فيروساً إلى شبكة الفضائيين لإنقاذ الأرض، لكن عندما سُئل عن البرمجية الخبيثة التي أصابت مركبة المحطة الفضائية أجاب المتحدث باسم ناسا "ليس هذا بالأمر الشائع، لكنها أيضاً لم تكن المرة الأولى".

في المستقبل القريب لن يكون على المجرمين والإرهابيين والناشطين

الإلكترونيين والحكومات المارقة، أن يسيطروا على الأقمار الصناعية للآخرين، بل سيتمكنون من بناء أقمارهم الصناعية الخاصة بهم. فثمة تقانات جديدة مثل أقمار كيوب ساتس المصغرة التي لا يتجاوز حجمها حجم علبة أحذية، ولا تكلف المليارات أو الملايين من الدولارات بل يمكن بناؤها وإطلاقها بكلفة لا تتجاوز مئة ألف دولار. ويمكن تشغيل هذه الأجهزة "خارج الشبكة"، بمعنى أنه يمكن إطلاقها والتحكم بها بعيداً من أنظار الحكومة، مما يفتح قنواتٍ لاتصالات الأقمار الصناعية الخاصة المشفرّة. وقد سبق لنادي كاؤوس للحاسب في برلين أن أعلن خطته لأخذ الإنترنت "بعيداً من مدى الرقابة، عبر وضع أقمار الاتصالات الخاصة بهم في مدارها"، وبينما من الواضح أنّ مستقبل استكشاف الفضاء يحمل معه فرصاً عظيمة للبشرية، إضافة إلى بعض المخاطر، فإنّ تقانات طوارئ أخرى على الأرض تتطلب مراجعةً أدق.

تقوم تقانة النانو على معالجة المادة على مستوى الذرات والجزيئات وصولاً إلى مرتبة النانومتر. ولفهم مدى صغر النانومتر، يكفي أن نفكر في أن قطر الشعرة البشرية ثمانية آلاف نانومتر. وثمة ثورةٌ تجري الآن مع سعي العلماء إلى خلق آلات على مستوى الجزيئات تستطيع القيام بأي شيء، من إصلاح أجسادنا إلى بناء حواسب فائقة السرعة. ففي عام 1991 نتج عن المراحل المبكرة من ثورة النانو شكل جديد من الكربون له بنية نانوية أسطوانية عرف بـ نانوكيوب، ولأسطوانات الكربون هذه خصائص مادية وكهربائية فريدة تجعلها أدوات فعالة على نحو استثنائي في تصغير حجوم الإلكترونيات. والغرافين هو مادةٌ نانوية أخرى تم اكتشافها عام 2004، وكان الأمل بها أن تكون عازلةً مثل البلاستيك تماماً. و"المادة العجيبة" أقوى بمئة مرة من الفولاذ وتزن سُدس وزنه وتنقل الكهرباء على نحو أفضل من النحاس، فربما تبنى الجسور والطائرات من هذه المادة يوماً ما، لكن

المرجح على كل حال هو أن يكون لها تأثير عميق على عالم الإلكترونيات. وفقاً للجمعية الأميركية للمهندسين الميكانيكيين، فإنّ تقانة النانو "لن تترك عملياً أي جانبٍ من جوانب الحياة دون أن تغيره، ويتوقع أن يشيع استخدامها بحلول عام 2020".

ربما كانت المساهمات الكبرى لتقانة النانو في مجال الطب، حيث يمكن لروبوت معالجة نانوي أصغر بآلاف المرات من الخلية السرطانية أن يدخل الدورة الدموية، حاملاً معه جزيئاتٍ من الذهب مُحملةً بعقاقير مضادة للسرطان لتوصلها مباشرةً إلى الموقع الدقيق للورم. علاوةً على ذلك، يمكن لتقانة النانو، كما هي حال البيولوجيا التركيبية، أن تستخدم كشكلٍ من أشكال المادة القابلة للبرمجة، أي المادة التي يمكنها تغيير خصائصها الفيزيائية كالشكل والكثافة والناقلية، بناءً على دخل المستخدم أو على استشعاراتها الذاتية. ويمكن أن تكون هذه المواد القابلة للبرمجة ذاتية التجميع كشرائط الحمض الريبي النووي، مُتبعَةً أسلوباً صاعداً من القاعدة إلى القمة تتبنى خلاله الجزيئات ترتيباً محدداً لها، وهو إنجازٌ يشيع تطبيقه في الطبيعة لكنه في المقابل بعيدٌ من متناول الهندسة البشرية.

مع أنها لا تزال في مرحلة الأبحاث والتطوير، فإن الآلات النانوية ستمكننا من خلق روبوتات نانوية، ما سيفرض تسارعاً على التغييرات الأسّية أساساً في حقل الروبوتات والذكاء الصنعي، لنصل إلى اليوم الذي سنخلق فيه روبوتاتٍ أصغر من خلايانا بألف مرة. سيكون لهذه الروبوتات النانوية آثارٌ هائلة في مجال الروبوتات، حيث ستتمكن من بناء أي شيء، من شرائح الصواريخ إلى الأجهزة الطبية القابلة للحقن، وسيكون لتقانة النانو آثر عميق على عالم المعالجة الحاسوبية أيضاً، حيث ستسمح لنا ببناء حواسب لها طاقات لا يمكننا تصديقها، حيث يمكن لحاسبٍ نانوي بحجم مكعب السكر أن يمتلك طاقة معالجةٍ تفوق كل ما يوجد في العالم اليوم.

لكن الأشياء الصغيرة تأتي بمخاطر كبيرةٍ جداً.

عُرف إريك دريكسلر بما طرحه في كتابه آلات الخلق عام 1986، من أنه إذا تمكنت الآلات النانوية (المُجمِّعات) من بناء المادة جزيئاً تلو الآخر، فإننا باستخدام الملايين من هذه المجمعات يمكننا بناء أية مادة وأي غرضٍ يمكننا تخيله. لكن للوصول إلى هذا المستوى، يترتب على العلماء أولاً بناء بعضٍ من المجمعات النانوية الأولى في المختبر، وتوجيهها ببناء مجمعات أخرى تقوم بدورها ببناء المزيد من المجمعات في عملية نموٍ أسّية مع كل جيل. وكان مصدر قلق دريكسلر من هذه الحالة هو أنها قد تخرج بسرعة عن السيطرة، حين تبدأ المجمعات بتحويل كامل المادة العضوية المجاورة لها إلى الجيل الجديد من الآلات النانوية في عمليةٍ اشتهر عنه تسميتها "سيناريو الهلام الرمادي"، الذي قد تنحسر فيه الأرض لتصبح كتلةً لا حياة فيها تسيطر عليها الآلات النانوية. فكيف يمكن لمثل هذا السيناريو أن يحدث؟ لنفترض أنّه تم في المستقبل إطلاق الملايين من الروبوتات النانوية لتنظيف بقعة نفطٍ كارثية في أحد المحيطات. قد يبدو الأمر عظيماً، باستثناء أن خطأً برمجياً صغيراً ربما يدفع الروبوتات النانوية إلى استهلاك جميع الأغراض الكربونية (من أسماك ونباتات وعوالق وحيود مرجانية)، بدلاً من استهلاك الهيدروكربونات الموجودة في النفط فقط. وقد تستهلك الروبوتات النانوية كل شيءٍ في طريقها "محولةً الكوكب إلى مجرد غبار". ولكي ندرك مدى سرعة حدوث ذلك، يمكننا تأمل المثال الذي ساقه دريكسلر في كتابه:

> تخيل مثل هذا المُضاعِف طافياً في قارورةٍ من الكيميائيات يستنسخ نفسه. سيقوم أول مُضاعِف بتجميع نسخةٍ عن ذاته خلال جزءٍ من ألف من الثانية، ثم سيقوم المضاعفان الناتجان ببناء مضاعفين آخرين خلال الجزء الثاني من

الثانية، ثم يبني الأربعة أربعةً أخرى ويبني الثمانية ثمانيةً أخرى. وفي نهاية عشر ساعات لن يكون لدينا 36 مضاعفاً جديداً بل أكثر من 68 ملياراً، وفي أقل من يوم واحد سيصبح وزنها طناً، وفي أقل من يومين ستتجاوز في وزنها وزن الكرة الأرضية، وبعد ذلك بأربع ساعات ستتجاوز كتلتها الشمس وجميع الكواكب مجتمعة، إلا إذا جفت قارورة الكيمياء قبل ذلك بوقتٍ طويل.

مع أن كثيرين قد استبعدوا سيناريو "الهلام الرمادي" معتبرين إياه خيالاً غير واردٍ على الإطلاق، فإنّ آخرين، ومن بينهم حكومات ومنظمات غير حكومية، أولوا هذا السيناريو اهتماماً جدياً مؤكدين أنّ بعض أشكال الحوادث لا يمكن للإنسانية تحمل تبعاتها ببساطة. بل إن دريكسلر نفسه وضّح في نهاية المطاف تعليقاته، مُهوناً من أمر الهلال الرمادي معتبراً إياه غير وارد. وسواءٌ حدث إطلاق غير مقصود لروبوتات نانوية قادرة على استنساخ نفسها أم لا، فإنّ قدرات هذه التقانة لن تفوت لاعبين خبثاء مثل المنظمات الإرهابية التي ربما تبدأ خلال عقدٍ أو أكثر في المستقبل باستكشاف أدواتٍ كهذه، تماماً كما فعلت عصابة أوم شنريكيو ضمن برنامج أسلحتها الكيميائية والبيولوجية في ثمانينيات القرن العشرين.

ثمة حقلٌ علمي ناشئ آخر ربما يحمل معه تحولاً هائلاً في مجال الحوسبة، هو ميدان الفيزياء الكوانتية. فعلى الرغم من وجود الكثير من العمل الذي لا بد من القيام به قبل أن تصبح الحوسبة الكوانتية حوسبةً سائدة، وعلى الرغم أيضاً من الكثير من الاختبارات التي أجريت على أنظمةٍ قائمة بينت أن الواقع لا ينطبق تماماً مع الآمال المعقودة، فإنّ الحواسب الكوانتية مؤهلةٌ لتنفيذ الحسابات بسرعاتٍ تجعل حواسب اليوم تبدو تافهةً. ففي أحد الاختبارات التي أجرتها غوغل وناسا، تمكّن حاسب كوانتي قيد

التطوير من تنفيذ عدة خوارزميات اختبارية بسرعاتٍ تفوق سرعة الطرائق الحاسوبية التقليدية بأكثر من 35 ألف مرة. الأمر الذي من شأنه أن يساعد في حل بعض أصعب المسائل في العالم، سواءٌ كانت البحث عن علاجات عقارية جديدة أم خلق الجيل التالي من التقانة النانوية أو الذكاء الصنعي.

حواسب اليوم ثنائية لا تمتلك لتنفيذ مجموعات تعليماتها سوى قيمتين ممكنتين، هما الصفر والواحد تمثّلان بواسطة ما يعرف باليِتّات. أما الحواسب الكوانتية، فتعتمد على خواص الجسيمات تحت الذرية، المعروفة بـ البتات الكوانتية أو الكيوبِتّات التي يمكنها أن تأخذ قيمة واحد أو صفر أو خليطاً منهما. المهم أنّ ذلك يسمح للحواسب الكوانتية باختبار عدد هائل من الإمكانات في الوقت نفسه، ما قد يكون له تأثيرات هائلة في مجال الأمن. بمزيدٍ من التحديد، تستطيع الحواسب الكوانتية القضاء على جميع أنظمة أمن الحاسب الشائع استخدامها اليوم قضاءً تاماً. حيث يعتمد أمن الحاسب حالياً على التشفير، أي استخدام نظرية العدد وعمليات ضرب الأعداد الأوليّة لتشفير الرسائل، بحيث تصبح غير قابلة للقراءة من قبل طرف غير مُرخص له. فلكي يتمكن شخص من قراءة بياناتك المشفرّة، عليه أن يمتلك المفتاح الرياضي أو أن يستخدم عملية "بحثٍ شامل" بتنفيذ العمليات الحسابية المطلوبة مراراً وتكراراً، لتحليل الأرقام الأوليّة المكوّنة للعدد المشفّر وصولاً إلى الحل الصحيح. فعندما ندخل كلمات سرنا، تقوم خوارزميات التشفير بتحويلها إلى العوامل العددية الصحيحة، لكي تفتح الرسالة وتخولنا قراءتها. ويعتبر هجوم البحث الشامل اليوم شيئاً لا يلجأ إليه القراصنة على الإطلاق، بل إنهم يعتمدون على وجود بروتوكولات تشفير ضعيفة التحقيق أو برمجيات حاسوبية خبيثة، أو برامج لتسجيل نقرات لوحة المفاتيح وعلى الأخطاء البشرية لسرقة مفتاح التشفير المطلوب لقراءة بيانات بطاقتك الائتمانية أو

معلوماتك المصرفية.

أما في حال عدم توفر كلمة السر الصحيحة، فسيضطر القراصنة إلى إجراء هندسةٍ عكسية على عملية التشفير، وهي عمليةٌ صعبة الحساب ويعتبر نجاحها غير واردٍ باستخدام حواسب اليوم. فحتى باستخدام حاسبٍ فائق سيستغرق هجوم بحثٍ شامل مليارات السنين لاختراق تشفير إيي.إي.إس المُرمز على 128 بتاً، والذي يعتبر اليوم معياراً سائداً في التشفير (يبلغ عمر الكون اليوم 13.75 مليار سنة فقط). بينما لا تستطيع الحواسب التقليدية تنفيذ أكثر من عملية حسابية واحدة في الوقت نفسه، تستطيع الحواسب الكوانتية تنفيذ عددٍ هائل من العمليات الحسابية بالتزامن. بعبارةٍ أخرى، من الممكن لحاسب كوانتي أن يتجاوز بروتوكولات التشفير ويسمح لصاحبه بقراءة البريد الإلكتروني لأي شخص، ومن تحويل الأموال من أي حسابٍ مصرفي وبالتحكم بأوراق المال وبالسيطرة على نظم التحكم بالملاحة الجوية، بالتلاعب بالبنى التحتية الحساسة. ومع أنك لن تستطيع أن تتناول واحداً من هذه الحواسب في متجر آبل في أي وقتٍ قريب، فإن الكثير من المنظمات في أنحاء العالم تعمل على بناء حواسب كوانتية قادرة على اختراق تقانة التشفير المتوفرة اليوم. وليس من المفاجئ أو أن ناسا قد قامت بالفعل بتخصيص 100 مليون دولار لتطوير "حواسب كوانتية مفيدة في التشفير" كجزءٍ من مشروع الأهداف الصعبة الاختراق. ولنكون واضحين، فإنّ هذه المسألة صعبة الحل إلى حدٍّ كبير، لكن أول شخصٍ يتمكن من حلها سيحوز في يده سلطةً هائلة، ولكنه ليس من الوارد أن يبوح بالأمر لكل أولئك الذين يقوم بقراءة اتصالاتهم والولوج إلى أنظمتهم.

إذا ما أخذت مجتمعة، تستطيع أقوى تقانات القرن الحادي والعشرين، بما فيها الروبوتيات والبيولوجيا التركيبية والتصنيع الجزيئي والذكاء الصنعي، توفير طاقةً كفيلةً بخلق عالمٍ من الوفرة والازدهار غير المسبوقين.

فمن مصادر الطاقة غير المحدودة إلى إنتاج موارد غذائية لا نهائية والتطورات الهائلة في الطب، يمكن للتقانات ذات التطور الأسّي أن تكون قوة خيرٍ استثنائية.

لكن ثمة جانبٌ مظلم لهذه التطورات أيضاً كما رأينا مرةً تلو الأخرى عبر صفحات هذا الكتاب. ففي عام 2000 بينّ بيل جوي، كبير العلماء السابق في شركة صن للنظم الصغرية، فكرةً عن المدى الذي يمكن أن تصل إليه الأمور نظرياً إذا ما ساءت الأحوال، في مقالةٍ مؤثرة نشرت في مجلة ويرد بعنوان "لماذا لا يحتاج إلينا المستقبل". وقد حذر جوي بشكل واضح من أن الروبوتيات والهندسة الجينية والذكاء الصنعي تهدد جميعها بجعل البشر "نوعاً مهدداً بالانقراض"، حيث ستستمر التقانات ذات النمو الأسّي في نموها إلى أن تتجاوزنا وتخرج عن سيطرتنا. ويشير جوي إلى أنّ جميع تقانات القرن الحادي والعشرين لدينا، تتم دمقرطتها وتتاح لأي شخص لديه اتصال بالإنترنت. فثمة نوادٍ لبناء الروبوتات في المدارس الثانوية ومنافسات في مجال البيولوجيا التركيبية في الجامعات. ويتولى الذكاء الصنعي قيادة سيارتنا، بينما يمكن شراء العربات المسيّرة على موقع كوستكو. إلا أنه بالمقارنة بالتهديد النووي، ثمة بونٌ شاسع مع توفر التقانات الأسّية النمو، بما لها من قوة تدميرية محتملة، على نطاقٍ واسع في متناول الشخص العادي اليوم. لكن هذا لا يعني أنه يجب حظر هذه التقانات ولا أن يوصد عليها في مختبرات الحكومة، نظراً لما يمكنها أن تقدمه من خير خصوصاً إذا ما تمت دمقرطتها. فمن منا يعلم من سيكون ذلك الطفل في جايبور الهندية أو تلك الجدّة في ملواوكي في ويسكنسون الذي سيحقق، أثناء عبثه في مجال البيولوجيا التجريبية، ذلك الفتح الكبير الذي سيغير قواعد اللعبة في مكافحة السرطان الذي لطالما أملناه به؟ لكنه من المحتمل بالقدر نفسه أن يكون بين هذه الجماهير بعض الأشرار الذين سيستغلون التقانات نفسها

لنشر وباءٍ عالمي وهو أمرٌ يدعونا إلى التوقف قليلاً، فعلينا التفكير بمزيدٍ من العمق والجديّة حول استخدامنا للتقانات ذات النمو الأسّي وبجوانبها المظلمة وبإمكانية أن تعود علينا بالأذى.

قد تكون الهجمات الفضائية والذكاء الصنعي الشرير والهلام الرمادي في نهاية قائمة أولوياتنا الشخصيّة، وفي موقع أدنى بكثير من عجلتنا لإحضار الأولاد من المدرسة. لكن ثمة كم هائل من التهديدات يتطلب انتباهنا الفوري، إذ تتعرض البنى التحتية الحساسة التي تشغل عالمنا، من شبكات الطاقة إلى أسواق المال، إلى هجومٍ مستمر ما يتركنا مع شبكة معلوماتٍ عالمية قد ينهار نظامها بسهولة. وفي الوقت نفسه، تتنامى حجوم البيانات التي ننتجها حول أنفسنا وحول الأشياء التي تحيط بنا بمعدلٍ آسّي، ما يفرض أسئلةً عميقةً حول خصوصيتنا وحول الآثار الأخلاقية لما أصبح ممكناً مع البيانات الكبيرة ومجتمع الرقابة الناشئ. فممن الممكن اختراق هذه البيانات وإعادة عرضها على عددٍ لا ينفك يتنامى من الشاشات التي تتكاثر في حياتنا، لتعرض علينا "حقائق" ليست في الحقيقة سوى أوهام. وما يزد الطين بلّة في ما يتعلق بالحوسبة التي لا يوثق بها، هو سهولة استخدام خوارزميات الصندوق الأسود لتحريف واقعنا بطرقٍ نكاد لا نتخيلها، إذ لا يعرف كُنهَ هذه الخوارزميات سوى من برمجها خلف أبوابٍ موصدة بعيداً من تدقيق العامة.

الحوسبة النقالة والإنترنت التي ينمو حجمها من حجم كرة غولف مجازية إلى حجم الشمس باتتا تلوحان في الأفق، وسرعان ما سيصبح بالإمكان وصل كل غرض فيزيائي بالإنترنت ومنحه عنوان إنترنت خاصاً به. لكن وجود مزيد من الأشياء على الإنترنت يعني وجود المزيد من الأشياء القابلة للاختراق، ما يمنح الأطراف الشريرة إمكانية الوصول إلى أجزاء أكثر وأكثر حساسية من حياتنا، من غرف نومنا إلى أجسادنا، مع تحول

البيولوجيا إلى جزءٍ متكامل من تقانة المعلومات. ومع كل خطوةٍ على هذه الطريق نجد المجرمين والإرهابيين والحكومات المارقة مستعدين لاستغلال غياب الأمن التقني الشائع لدينا عبر ثغرات لا تنتهي في البرمجيات والعتاد الحاسوبي اليوم. ويمتاز عاملو المعرفة غير الشرعيين هؤلاء في القرن الحادي والعشرين بإبداعٍ عميق وقدرةٍ على التأقلم، وهم يدأبون على التعلم وعلى تبني آخر المنهجيات التجارية، من التعهيد الجماعي إلى برامج المشاركة التسويقية لتدمير التقانات التي تحيط بنا.

من شأن التطورات التي يتم تحقيقها في مجال الحوسبة والذكاء الصنعي أن تجعل الجريمة عبارةً عن مهمة تنجز بواسطة البرمجيات الخطاطيّة والخوارزميات، ما يمنحها فعاليةً أكبر ويقلل من حاجتها إلى البشر لارتكابها. والأسوأ من ذلك هو أنّ الأدوات المتوفرة لدينا للكشف عن مثل هذه التهديدات غير مناسبةٍ على الإطلاق، فمع مرور 95 بالمئة من تهديدات البرمجيات الخبيثة الجديدة دون اكتشافها ومع وصول وقت اكتشاف متسللٍ إلى الشبكات التجارية إلى نحو 210 أيام، من الواضح أنّ أياً من أنظمتنا يمكن اختراقه عند الرغبة من قبل من يتوفر له الوقت والدافع لفعل ذلك. بل إن ذلك لا يتطلب الكثير من الوقت، كما بينت دراسة أجرتها خدمة فيريزون سِكريت، فـ 75 بالمئة من جميع أنظمة الحاسب يمكن اختراقها خلال بضع دقائق فقط، بينما يتطلب 15 بالمئة منها فقط أكثر من بضع ساعات لاختراقه.

سيكون أثر مثل هذه التهديدات أوضح بكثير مع تحول الجريمة السايبرية إلى ثلاثية الأبعاد، ومع دخول مليارات الأغراض الجديدة إلى إنترنت الأشياء، ومع ظهور عالمٍ شبكي جديد قابل تماماً للاختراق. بل وربما يكون أقل أماناً من حواسبنا المحمولة وهواتفنا الذكية المتوفرة الآن. تشير المخاطر التي تنطوي عليها الحوسبة الثلاثية الأبعاد المتمثلة في ظهور الروبوتيات، إلى أننا

نقوم بصنع آلاتٍ تمتلك القدرة على التفوق علينا وتجاوزنا في طاقاتها وتمتلك قوةً أكبر بعد من خلال قدرتها على العمل في جماعات أو كأسراب لتحقق أهدافها. وهي فكرة مقلقة إذا ما نظرنا إلى المهارات المادية المتزايدة للجحافل المتكاثرة من الروبوتات العسكرية الطائرة والسائرة والسابحة، المزودة في معظمها بنظم ذكاء صنعي توجهها، ومع تزويد بعضها باستقلالية قاتلة لاتخاذ "قرارات قتل" لصالحنا. إنّ التهديد السايبري يتحول بذلك من مجرد مشكلةٍ افتراضية إلى خطرٍ يتهدد العالم المادي. والنتيجة هي، كما رأينا عبر هذا الكتاب، إلى أن الخيال العلمي يتحول إلى واقعٍ علمي أمام أعيننا.

مع ظهور الإنترنت ومع الوصول الوشيك لمليارات الاتصالات الإضافية التي ستصبح ممكنةً بفضل إنترنت الأشياء وحساساته، تمكن كوكبنا من تطوير نظامٍ عصبي لا ينفك يتوسع. فهو يربط اتصالاتنا وأفكارنا، بل حتى أجسادنا، إلى دماغٍ عالمي شبكي ذي تعقيدٍ هائل تتحكم به مجموعةٌ كبيرة من النظم البرمجية والبروتوكولات الشبكية، من الواضح أنّه من الممكن استغلال أي منها من قبل أولئك الذين يودون إلحاق الأذى بنا. ومن المؤسف أن نظام المناعة الذي يحمي هذا النظام العصبي العالمي نظام ضعيف يتعرض لهجوم مستمر، سيكون لانهياره تبعات تفوق خيالنا. والنتيجة أنّه قد حان الوقت للبدء بتصميم وهندسة وبناء نظمٍ أكثر متانةً للحماية الذاتية، تكون حارستنا القادرة على النمو والتأقلم بسرعةٍ وتواكب سرعة ظهور التقانات الجديدة في عالمنا. فعلى الرغم من سهولة التركيز على المنافع الوفيرة التي تعود بها التقانة على حياتنا فقط، نجدنا نتجاهل المخاطر التي ترافقها وتحيق بنا.

إننا اليوم نعيش في عصرٍ يشهد نمواً أسّياً، بينما لا نزال فيزيولوجياً بأدمغةٍ تعود إلى صيادي العصر الحجر بالكاد تطورت خلال السنوات الخمسين ألفاً

المنصرمة. أي إنه ليس من طبيعتنا مواكبة الطاقة التي تحملها التقانات الأسّية. لكن لا بد لنا من أن نحاول. فتماماً كالمخلوقات التي تعيش في مستنقعٍ تحت أوراق الزنبق المائي، والتي ضربنا بها مثلاً في ما سبق، فكانت تحت تهديد تغييرٍ أسّي، حالها هو حالنا. فالطلاب الذين تم تحذيرهم في فرنسا كان لديهم ثلاثون يوماً ليتصرفوا وينقذوا البركة، لكنهم في اليوم الخامس والعشرين لم يرو أي شيء يثير قلقهم، لأن الزنبقة المائية لم تكن تغطي سوى 3 بالمئة من سطح البركة فتركوها تنمو. لكن كما نعلم، وبحلول اليوم التاسع والعشرين، كانت الزنبقة المائية قد نمت نمواً مذهلاً لتغطي نصف البحيرة. لكن بحلول ذلك اليوم، كان هنالك القليل الثمين من الوقت لإنقاذ البركة التي لم تلبث أن خنقتها الزنبقة في اليوم التالي بالذات. قد يبدو من السهل تجاهل انعدام الأمن في تقاناتنا اليوم بجملتها. فمن الممكن بلا شك أن تُخترق بضعة ملايينَ من الحسابات هنا، وأن تسرق بضعة مليارات من كلمات السر هناك، لكن لا يزال لدينا الوقت. لقد تم اختراق الطائرات المسيّرة والمنظِّمات القلبية ونظم الملاحة الجوية والسيارات وأضواء الشوارع ونظم الملاحة وآلات التصوير بالرنين المغناطيسي، لكن لا يزال لدينا وقت. ثمة عشرات المليارات من الأغراض الجديدة التي ستضاف إلى الإنترنت، لكن لا يزال لدينا وقت. أليس كذلك؟

أمارات الخطر باتت واضحة. فالتقانة تجعلنا أكثر تواصلاً وتابعيةً وعرضةً للخطر. ومع أن هذه الوفرة من الفتوحات العلمية التي أصبحت ممكنةً بفضل التقانة الأسّية تَعِدُ بمنافع عظيمةٍ غير مسبوقة تعود بها على البشرية، فإنّه لا بد من توجيهها وحمايتها من أولئك الذين يريدون استغلالها لإيذاء الآخرين. ونحن حين نتجاهل الدليل الدامغ على المخاطر التقانية التي تحيط بنا، إنما نفعل ذلك على مسؤوليتنا، فاليوم التاسع والعشرون يقترب بسرعة. فما الذي سنفعله حياله؟

الجزء الثالث

تقدم البقاء

الفصل السابع عشر
النجاة في زخم التقدم

بالنسبة لي، أن أفهم الكون كما هو، لأفضل بكثير من أن أصر على الوهم، مهما كان مُرضياً ومطمئناً.

كارل ساغان

كانت رحلةً صعبة، طُلب منا خلالها التفكير بأسئلة صعبة وغير مريحة أحياناً حول التقانة ودور الأجهزة كلية الوجود في حياتنا، تلك الأجهزة التي رحبنا بوجودها في منازلنا ومكاتبنا ومدننا، بل في أجسادنا، من دون سؤال. لقد علمتنا هذه الرحلة أن ننظر بدقة وتشكك إلى العدد المتزايد لشاشات الحاسب التي تتكاثر في عالمنا، شاشات أدرناها 180 درجة لنرى الجانب الآخر من الحكاية، الخوف من الخطر جنباً إلى جنب مع التفاؤل في قصة حبنا للتقانة. واتصالنا المتزايد ببعضنا إلى جانب انتشار أنظمة الحوسبة الضعيفة بطبيعتها، يعني أن عاصفة انعدام الأمن التقاني لم يعد بالإمكان تجاهلها بعد الآن.

لا تكمن المشكلة في أن التقانة سيئة بالطبع، بل في أن قلة قليلة تفهمها. إذ يمكن تخريب الشيفرة الحاسوبية التي تدير كوكبنا لتستخدم ضدنا من قبل أولئك الذين يصلون إليها. والأزمنة الأسية تقود إلى جرائم أسية، جرائم يتمكن فيها أفراد معزولون مريضو النوايا من الوصول والتأثير سلباً على عشرات ملايين الأشخاص، في أي مكان وفي أي وقت. بالفعل، فإن قطاع البنى التحتية للمعلومات الحساسة الذي يدير مجتمعنا معرض برمّته للخطر. وتزداد خطورة هذه التحديات بشكل كبير عندما تتصل مليارات الأشياء الجديدة بالإنترنت، وتبدأ أجهزة الحاسب المتشابكة على شكل روبوتات بالتحرك في الفضاء المادي الذي ستتشاركه معنا، ناهيك بالمخاطر الناجمة عن الذكاء الصنعي والبيولوجيا التركيبية. ويبدو الأمر بمجمله شاقاً

ومربكاً، ولكن إنجاز التغيير المطلوب لتعزيز الأسس المستقبلية لتقانة الغد يبدأ بفهم وإدراك هذه التهديدات.

لا توجد إصلاحات سهلة للحالة التي نحن فيها حالياً. ولا يوجد ترياق أو حل واحد يجعل الأمور أفضل وكأن كل ما علينا هو أن "نضيف الماء للمزيج فقط". فمليارات الخطوات الفردية قادتنا إلى هذا المأزق، وقد يتطلب إخراجنا منه مليارات أخرى. ونظراً للطبيعة المتباينة للتهديدات، فإن كل ما يحتاج إليه المهاجمون هو أن يجدوا نقطة ضعف وحيدة فقط، بينما على المدافعين أن يصدوا كل الهجمات الممكنة، وهو أمر مستحيل في الحقيقة. بالرغم مما سبق، نحن لم نفقد كل شيء بعد، والأمور لم تصبح ميؤوساً منها. فنحن لا نحتاج لـ "أمان تام" ولن نحصل عليه، فلا وجود لشيء كهذا. لكن الغياب شبه الكلي للحوسبة الموثوقة في عالمٍ تديره أجهزة الحاسب يجب أن يكون ضوء إنذارٍ أحمر يومض لنا جميعاً.

لا شك في أن للعلم والتقانة نتيجة إيجابية للبشرية في المحصلة. ولكن إذا كنا نريد الازدهار والتقدم في القرن المقبل، فعلينا أن نتغلب على المخاطر التقنية التي تترافق حتماً مع هذا التقدم. ثمة خطوات يجب أن نقوم بها اليوم، وتصحيحات لا بد منها لمسارنا لدرء خطر المستقبل الذي يلوح في الأفق أمامنا. في الصفحات التالية، هناك مجموعة متنوعة من النصائح التكتيكية والاستراتيجية التقنية والتنظيمية والتعليمية، وأخرى متعلقة بالسياسة العامة تهدف إلى تقليص المخاطر المتنامية التي تفرضها التقانة. وأنا أعتقد أن التالي هو الأهم من بين الخطوات التي يجب علينا اتخاذها لحماية مستقبلنا التقاني. وقد وُجدت التقانة لتستمر، فلا عودة للوراء. لكن السؤال الحاسم هو كيف سنستخدم هذه الأدوات لتحقيق أكبر فائدة ممكنة مع تقليص سلبياتها. فإليكم كيف يمكن لنا أن ننجو في زخم هذا التقدم.

كل تحديث أمني تجريه... يعني أن الشيء الذي تم تحديثه، أياً كان، كان معطلاً، يقبع ضعيفاً لا أحد يعرف منذ متى. أيام ربما، وسنوات أحياناً.

كوين نورتن

عمل مطورو البرمجيات لدى فايسبوك لزمن طويل تحت شعار "تحرك بسرعة واكسر الأشياء". وتعكس هذه المقولة التي كتبت على الجدران في مقر الشركة الرئيسي روح الاختراق لدى فايسبوك، والتي تقول بأنه حتى إذا لم تكن الأدوات أو الخصائص البرمجية الجديدة مثالية، فإن سرعة ابتكار الشفرات هي المعيار، حتى لو تسبب ذلك بمشاكل أو مسائل أمنية مع الوقت. ووفقاً لزوكربيرغ فإنك "إذا لم تكسر شيئاً، فأنت لا تتحرك بسرعة كافية على الأرجح". وليس الفايسبوك هو الوحيد الذي يقوم بسياسات كتابة البرمجيات على هذا النحو. فالأغلبية العظمى من الشركات العاملة في مجال البرمجيات تعمل تحت مجموعة متنوعة من الشعارات مثل "اشحنه فقط" و"المنجز أفضل من المثالي"، سواء في العلن أو وراء الأبواب المغلقة. ويعترف العديد من المبرمجين بقيامهم بشحن برمجيات يعترفون بأنها "رديئة" ولكنهم لا يأبهون لذلك، على أمل أن يقوموا، ربما، بعملٍ أفضل في المرة القادمة. تلخص هذه المواقف كل المشاكل التي تعانيها عملية كتابة برمجيات، ولعلها تمثل الخطر الأكبر الذي يتهدد أمن الحواسب اليوم.

قد يفاجأ عامة الناس إلى حد كبير بقدر التقانة الذي بالكاد يعمل من حولنا، مزدانة بما يسمى "برمجيات الترقيع" التي لا يفصلها عن انهيار النظام سوى بضع ضربات على لوحة المفاتيح. كما أشار الصحافي "كوين نورتون" الذي يعمل لمجلة وَيَرْد ويغطي أخبار أوساط القراصنة، فإن "البرمجيات هي هراء". فمعظم المبرمجين محملون أكثر من طاقتهم

وينقصهم المال والوقت. فهم أيضاً يريدون العودة للمنزل فقط ورؤية أطفالهم، وما نحصل عليه بالمحصلة هو برامج غير مكتملة مليئة بالعيوب والثغرات الأمنية التي تعصف بها الرياح وتتعرض باستمرار لحوادث مثل ثغرة "هارت.بليد" (القلب النازف)، أو الهجمات الضخمة على شركات تارغت وسوني بلاي ستايشن وهوم ديبوت.

لم تعد كتابة الشيفرات الحاسوبية اليوم بالعمل السهل، بل باتت عملاً معقداً إلى حد لا يصدق. فهناك نحو خمسين مليون سطر كامل من الشيفرات الحاسوبية في حزمة مايكروسوفت أوفيس لوحدها، يجب أن يعمل كل منها بشكل مثالي إذا ما أريد لهجمات المخترقين أن تُكبح. ولكن لا بد للأخطاء من أن تحدث بالطبع. وهذا برنامج واحد فقط، بينما على حاسبك أو هاتفك الذكي أن يراقب ويحقق الانسجام بين كل البرامج التي يقوم بتشغيلها، ناهيك بالبرامج التي تعمل على أنظمة أخرى ويرغب جهازك بالتفاعل من خلالها مع كل موقع إلكتروني تزوره. وتتفاقم المشكلة بشكل كبير مع ازدياد عدد أجهزة إنترنت الأشياء التي بدأت بالتواصل بعضها مع بعض. فلكل الثغرات والعيوب الأمنية الموجودة في البرمجيات فعل تراكمي يظهر على شبكة المعلومات العالمية لدينا. لذا السبب يمكن اختراق 75 بالمئة من أنظمتنا خلال بضع دقائق. لقد دفع هذا التعقيد المصحوب بأسلوب "دعه يعمل" المتبع بشكل كبير مع الثغرات البرمجية بالباحث القدير في مجال أمن أجهزة الحاسب دان كامينسكي إلى القول بأننا اليوم "نعيش بحقّ حالة البرمجة في زمن الكوليرا".

ويرد العديد من المبرمجين عند سؤالهم عن الحالة السيئة للبرامج في العالم اليوم بالحجة التالية: "نحن لسنا سوى بشر، ولا يوجد شيء اسمه البرنامج المثالي". وهم محقّون في ذلك. ولكننا لسنا قريبين حتى من الحالة المثالية، فوفقاً للباحث الأمني القدير شارلي ميلر، نحن لم نحقق سوى 50

بالمئة مما يمكن ويجب تحقيقه، ومن شأن رفع هذا الرقم إلى 70 أو 80 بالمئة أن يسبب تغيراً كبيراً في أمن الحاسب ككل. فالمستهلكون يرغبون ببرامج فعالة وغنية بالميزات، ويريدونها الآن. فعشرات الآلاف مستعدون للوقوف في صفوف الانتظار لأيام، والنوم على أرصفة الطرقات، للحصول على أحدث آخر هاتف آيفون. لكن على مزودي البرامج أن يقوموا بتحسين لعبتهم وأن يفكروا في تصميم الحلول الأمنية منذ البداية كمكوّن مفتاحي للحوسبة الموثوقة، وأن يبدأوا بالأسس التي سيتم البناء عليها.

لكي نغير وجهة الدفّة، لا بد من توجيه الحوافز باتجاه ضمان التشديد على الحاجة الملحة لأمن الحوسبة. على سبيل المثال، عندما يجد المخترقون اليوم نقطة ضعف في أحد البرامج، يكون أمامهم إما بيعها في السوق السوداء لشركة الجريمة بمبلغٍ معين أو إبلاغ البائعين عنها مقابل لا شيء، بل مع خطورة التعرض للملاحقة القانونية. لذا فإنهم يتخذون الخيار الواضح. ومع أن الأمور بدأت بالتغير، فقد أنشأت بعض الشركات "برامج مكافأة لصيد الثغرات الأمنية"، إلا أن قلة منها تعرض مكافأة نقدية، وحتى أولئك الذين يعرضون المال، تبقى عروضهم أقل بكثير من العروض المتاحة في العالم السري الرقمي. على هذا أن يتغير، فتطوير برامج جيدة التمويل للتبليغ عن نقاط الضعف الأمنية تدفع المخترقين إلى تنبيه الباعة إلى العيوب الكبيرة سيساعد على تقليص الضرر الذي سببته شركات البرمجة لنفسها عندما استعجلت بإنتاج برامج غير آمنة مليئة بالثغرات وقدمتها لعامة الناس الغافلين.

نظراً لكون البرمجيات هي المحرك الذي يدير الاقتصاد العالمي وجميع البنى التحتية الحساسة لدينا، من الكهرباء إلى نظام الهاتف، فليس هناك وقت نضيعه. لكن الأمر يحتاج لما هو أكثر من مجرد بضعة باحثين أمنيين يكتبون مقالات مقنعة حول الموضوع؛ إذ يتطلب احتجاجاً من العامة

للحصول على برامج ذات جودة أفضل، وهو ما لا يزال غائباً حتى هذه اللحظة. فكر بالأمر، لماذا نقبل بكل هذه العيوب وكأنها الحالة الطبيعية؟ ليس بالضرورة أن تكون الحال على هذا النحو. يمكننا أن نحدث التغيير عندما نعتبر المسؤولين عن قطاع البرمجيات، الذي تبلغ قيمته 150 مليار دولار في السنة، مسؤولين عن أفعالهم. أما عند غياب مطالب العامة في المعركة الدائرة بين الأرباح والأمان، فإن الأرباح هي التي ستفوز في كل مرة. علينا أن نجعل الشركات تدرك أن كتابة برامج أكثر أماناً هو أمر لصالحها على المدى البعيد، وأن هناك عواقب تنتظرها عند فشلها في ذلك. أما في حالنا اليوم، فلا يحمل المهندسون والمبرمجون والشركات المسؤولة عن ابتكار تقانة اليوم أي مسؤولية مهنية أو شخصية تقريباً عن أفعالهم. لقد حان الوقت لتغيير ذلك.

أضرار البرمجيات

ذكر بروفسور جامعة يال المعروف في مجال علوم الحاسب إدوارد توف ذات مرة أن هناك مجالين من الأعمال يشيران لزبائنهما كـ "مستخدمين": مصممو برامج الحاسب وتجار المخدرات. والأهم من ذلك هو أن فرصة تعافيك من الأضرار التي تسببها منتجاتهما واحدة. فحقيقة الأمر هي أنك عندما تضغط على زر الموافقة على قائمة شروط الخدمة الطويلة دون أن تقرأها، فأنت توافق على استخدام برامج الشركة أو خدمات الإنترنت كما هي، وتقع عليك كامل المسؤولية عند حدوث أي ضرر. تستخدم هذه الشركات لغة مثل "سوف تتعهد بعدم إلحاق الضرر وبتبرئة ذمتنا نحن وشركاؤنا ومسؤولونا وعملاؤنا وموظفونا من أي شكوى أو فعل أو دعوى تنتج عن أو تتعلق باستخدام الخدمات" و"نحن لا نضمن أن منتجنا سيكون آمناً أو مضموناً أو خالياً من الأخطاء دائماً". هل ستشتري شطيرة شيبوتل بوريتو لو رافقها مثل هذا التحذير؟ لا أعتقد ذلك. إذاً، كيف

تمكنت تجارة البرمجة من خلق مثل هذا الاستثناء لنفسها بحيث لا تكون مسؤولةً عن أي شيء؟ إنه سؤالٌ جيد.

عندما تتعطل سيارة بسبب توصيل خطأ للأسلاك أو وجود برمجيات ثابت رديئة، كما رأينا في حالات التسارع المميت لسيارة تويوتا، يمكن لهؤلاء المتضررين أن يرفعوا دعوى بسبب الأضرار. فلِمَ لا يحدث ذلك مع البرمجيات؟ هل من المنطقي أن نقترح أنه عندما يموت أحدهم أو يعاني خسارات اقتصادية ضخمة بسبب لبرمجيات خطأ أن يُحرم هذا الشخص أو أحباؤه رفع دعوى لأن شروط الخدمة تفرض ذلك؟ حتى عندما يمكن أن نثبت للقضاة والمحلفين أن البرنامج هو المسؤول المباشر عن إلحاق الضرر؟ لا أعتقد ذلك.

أرجو ألا يساء فهمي. فأنا لست من المعجبين باختراع القوانين الجديدة التي لا هدف منها. ولا أود أن اقترح أن القوانين هي المقاربة الفضلى للتعامل مع انعدام الأمن الذي يشمل عالمنا الافتراضي. فهي في أفضل الأحوال أداة حادة في مجال يتطور بشكلٍ سريع كالتقانة. ولكن يجب رسم خط ما في الرمال. فالتجاهل الطائش لأي من، أو لكل، العواقب التي تنتج عن البرمجيات الرديئة، والتي يتم نشرها مع العلم بنقاط الضعف الموجودة فيها وتقديمها إلى الناس العاجزين عن قراءة ملايين السطور من الشيفرات البرمجية على هواتفهم الذكية أو حواسيبهم الشخصية بمفردهم ليقدّروا المخاطر المترافقة، لهو خطأ فادح. فعلى هؤلاء الذين يبتكرون ويكتبون هذه الأدوات أن يتحملوا بعض المسؤولية.

من نافل القول إن تجارة البرمجيات تعارض بشدة أي تغيير من هذا القبيل. فهي تدعي أن السماح بدعاوى المسؤولية سيكون له آثار كارثية على أرباحها وقد يسبب إفلاس هذا القطاع. كما أنها تؤكد أن تعقيد التفاعلات البرمجية هائل إلى حد يستحيل معه إصدار حكم بالمسؤولية في

حال حدوث ضرر. كلتا الحجتين ضعيفتان. وقد سبق لنا أن مررنا بهذا كله في السابق، وخاصة مع تجارة السيارات التي كانت منتجاتها حتى الستينيات حافلة بسجل أمان مرعب. فقد تم تمرير القانون الوطني لسلامة المركبات والمرور في الكونغرس عام 1966 من خلال حملات الدفاع عن المستهلك والعمل، ليسمح للحكومة بفرض قوانين السلامة الخاصة بهذا القطاع. ونتج عن ذلك أحد أعظم الإنجازات في مجال الصحة العامة في القرن العشرين. حيث انخفضت نسبة الوفيات الناتجة عن السيارات بسرعة، وأُنقذت عشرات الآلاف من الأرواح.

قد تكون تقانة اليوم أكثر تعقيداً من سيارات الأمس بالطبع، ولكن لن يكون هناك تحسن في أمان وسلامة برمجياتها ومنتجاتها إلا عندما يتم توجيه الحوافز باتجاه تشجيع حدوث التغيير. إن أي ضرر يعانيه المستخدمون النهائيون يقع حالياً على عاتقهم، وعلى عاتقهم وحدهم، مع وقوع القليل من الضرر على الباعة في أحسن الأحوال. فثمة القليل من العواقب، إن وجدت، لبيع الشيفرة البرمجية الرديئة، لذا فإن هذه الممارسة تستمر بدون انقطاع. ولن يحدث التغيير ما دام هؤلاء المسؤولون عن المشاكل الأمنية الكامنة لا يُحاسبون على أفعالهم. فعندما تصبح التكلفة التجارية لإصدار برمجيات دائمة التعطّل أكبر من كلفة إصلاح نقاط الضعف المعروفة منذ البداية، عندها فقط ستميل دفة الميزان لمصلحة برامج أفضل وأكثر أماناً. ومع أنني لست أدافع عن إنشاء منظومة جديدة من القوانين والبيروقراطيات الحكومية، فإنني اعتقد بأنه لا بأس بنقاش عام قوي حول الأسباب الكامنة وراء المشاكل الأمنية الحاسوبية واسعة الانتشار. لقد حان الوقت الآن لكي نقوّم أنظمتنا وبرامجنا المنزلية قبل أن نضيف خمسين مليار شيءٍ جديد إلى شبكة المعلومات العالمية التي لدينا.

تقليص تلوث البيانات واستعادة الخصوصية

عبر صفحات هذا الكتاب، رأينا عواقب تكديس البيتابايتات من البيانات والمعلومات التي لا تلبث أن تتسرب في النهاية. وسواء كانت سجلات طبية شخصية أم حسابات مصرفية أم أسراراً حكومية أم ملكية فكرية تجارية، مآل جميع هذه البيانات هو إلى التسرب. وتخزين هذه البيانات الضخمة ووضعها بيد حفنة من شركات البيانات والإنترنت الكبرى يجعلاها صيداً ثميناً تصعب مقاومة مهاجمته وسوقاً مستمرة للصوص. وكما قلت في السابق، كلما زاد إنتاجك من البيانات، زاد حجم الجريمة المنظمة الراغبة باستخدام هذه البيانات.

بينما اختار معظم مستخدمي الإنترنت طواعية أن يشاركوا بعض التفاصيل الأكثر حميمية في حياتهم عبر الشبكات الاجتماعية، تقوم الشركات المسؤولة عن هذه الخدمات بجمع معلومات أكثر بكثير مما ندركه. ولا ينفك مزودو خدمات الإنترنت "المجانية" يتعقبون المستخدمين عبر كامل رحلتهم على الشبكة، بل خلال تحركاتهم في العالم المادي بينما يستخدمون هواتفهم النقالة. ولكن، وكما سبق ورأينا، فإن أغلى الأشياء في الحياة مجانية. إذ يتم تقسيم كل هذه المعلومات وتقطيعها في شرائح أو مكعبات وبيعها في عالم مظلم سري يحكمه سماسرة البيانات، الذين قلما يهتمون أو يراقبون دقة المعلومات التي يحتفظون بها أو أمانها. ومع أننا قد نشتكي هذه الممارسات (إذا كنا المستهلكين الفعليين لدى شركات الوسائط الاجتماعية هذه)، فإننا عاجزون عن ترجمة هذه الشكاوى إلى واقع. لقد قايضنا هذه الحقوق ببريدٍ إلكتروني وتحديثات للحالة وصور مجانية على الإنترنت، وعبرنا عن موافقتنا على ذلك عندما ضغطنا زر الموافقة على اتفاقية شروط الخدمة، المؤلفة من خمسين صفحة بحروف دقيقة لا يقرأها أحد منا. هذه "الاتفاقيات" المخادعة المبرمة كلياً من طرف واحد، لا ينبغي أن تبرئ الشركات التي تفرضها من كامل المسؤولية المتعلقة

بكيفية حفظها وتخزينها لبياناتنا. فإذا اختاروا أن يحتفظوا بكل تفصيل صغير يمكن لهم أن يجمعوه عن حياتنا، فإن عليهم أن يكونوا مسؤولين عن التبعات.

ما يشكل صدمة في هذا النظام هو أنه لا داعي لأن يكون مصمماً بهذه الطريقة. إذ تشير التقديرات إلى أن كل مستخدم للفايسبوك يولد نحو 8 دولارات كعائدات من الإعلانات (بدون أرباح) للشركة سنوياً. لكنني سأفضل أن أرسل 10 دولارات للشركة على أن تدعني وشأني. فهذا المبلغ، الذي لا يتجاوز الدولار الواحد في الشهر، هو أقل بمئة مرة من فاتورة تلفزيون الكابل. إنه نظام مختلّ بأكمله. وكما أعلن الباحث إيثان زوكرمان في معهد ماساتشوستس للتقانة، "الإعلانات هي الخطيئة الأصلية للإنترنت. فالحالة المتدهورة للإنترنت هي نتيجة مباشرة، إن لم تكن مقصودة، لاختيار الإعلانات كنموذج افتراضي لدعم المحتوى والخدمات على الإنترنت". رغم أن بياناتنا تدر المال اليوم على مواقع جيميل ويوتيوب وفايسبوك، يمكننا بالسهولة نفسها أن ندعم الشركات التي تهدف إلى تخزين أقل قدر ممكن من المعلومات الشخصية، مقابل مبالغ زهيدة من المال. فلِمَ لا نقوم بحذف الوسيط تماماً لنحصل على نظام أكثر منطقية؟ عندها سنصبح زبائن لدى جوجل وفايسبوك مقابل دولار واحد في الشهر وسنصبح قادرين على الاستمرار والاستمتاع بحياتنا.

لسوء الحظ، وتماماً كما هي الحال مع بائعي البرمجيات، يتم اليوم توجيه الحوافز خطأً بعيداً من منظور الأمن والسلامة العامة. لقد تم تحفيز فايسبوك على جمع كمية متزايدة من البيانات الشخصية عن مستخدميه بحيث يمكنه بيعها لآلاف سماسرة البيانات حول العالم لتحقيق الربح. هذا هو نموذجه التجاري. أما ما إذا كان من يشتري هذه المعلومات يسمح باستخدامها في النهاية في عمليات انتحال الشخصية أو المطاردة أو

التجسس الصناعي، فهذا آخر ما يهم شركات الوسائط الاجتماعية بعد بيعها للمعلومات بالمزاد العلني لصاحب العرض الأفضل. لكن الأمر يهمنا بالطبع، نحن الذين نعاني الأضرار الاقتصادية والاجتماعية لتسرّب هذه البيانات. فلنترك أولئك الذين يفضلون حسنات النظام "المجاني" يستمتعون به وبكل تبعاته. فلماذا لا يتم منح بقيتنا خيار دفع المال مقابل الحفاظ على خصوصيتنا وأمننا؟

بينما قد يبدو من المستحيل أن "نعيش خارج الشبكة" في عالم اليوم الحديث، يمكننا أن نصمم نظاماً أكثر أماناً بشتى الوسائل. وهناك أمثلة أفضل وأكثر توازناً حولنا، مثل تعليمات حماية البيانات في الاتحاد الأوروبي، والتي تعتبر سهلة الاستخدام كما أنها تقدس الخصوصية كحق أساسي لجميع مواطني الاتحاد الأوروبي. فهي تقوم بتحديد ما يمكن لشركات البيانات أن تخزنه عنا والمدة الزمنية التي يمكن لهذه الشركات أن تحتفظ خلالها بالبيانات قبل أن يتوجب حذفها. إنها مقاربة أكثر عقلانية لا تقوم فقط بضبط ميزان القوى المنحرف كلياً في ما يتعلق بعلاقتنا بشركات الإنترنت، بل تحمينا وتحمي بياناتنا من التسرب والوصول لأيدي شركة الجريمة أيضاً.

نهاية كلمة السر

كما رأينا في الفصل الأول مع الاختراق الملحمي الذي وقع ضحيته مات هونان، لم تعد هذه السلسلة من الأحرف والأرقام قادرة على حمايتنا. يمكنك بالطبع شراء بعض الوقت عبر ابتكار كلمة سر مؤلفة من خمسةٍ وعشرين حرفاً مع أحرف صغيرة وكبيرة ورموز وأرقام، ولكن حقيقة الأمر هي أن أحداً لا يفعل ذلك. فبدلاً من ذلك، وحتى في عام 2015، تبقى كلمات السر أكثر شيوعاً هي "123456" و"كلمة سر". إذ يقوم خمسة وخمسون بالمئة من الناس باستخدام كلمة السر نفسها عبر أغلب المواقع

الإلكترونية، ولا يكلف أربعون بالمئة أنفسهم عناء إعداد كلمة سر على هواتفهم الذكية. وحتى حين يفعلون، فإن ذلك قد لا يساعد كثيراً. فنظراً للتطور الحاصل في قوة الحوسبة والمعالجة السحابية والبرمجيات الإجرامية في العالم السري الرقمي، فإن أكثر من 90% من كلمات السر يمكن فكها وكسرها خلال عدة ساعات فقط، كما تبين دراسة قامت بها شركة ديلويت للاستشارة. والأسوأ من ذلك هو أن منظمات شركة الجريمة، مثل سايبر فور الروسية، جمعت أكثر من 1.2 مليار اسم مستخدم وكلمة سر يمكنها استخدامها لفتح الحسابات عند رغبتها. فمن الواضح تماماً أن نظامنا الحالي المعتمد على اسم مستخدم وكلمة سر فقط فاشل كلياً.

ثمة بعض الإجراءات التي يمكننا اليوم أن نقوم بها لتزودنا بطبقات مختلفة من الحماية. مثال ذلك التحقق المزدوج من الهوية الذي تقدمه مواقع غوغل ومايكروسوفت وبايبال وآبل وتويتر وغيرها، والذي يجمع بين اسم المستخدم وكلمة السر مع شيء آخر تملكه كرمز أمان أو مفتاح السيارة أو الهاتف المحمول. وتستخدم معظم شركات الإنترنت للمستهلك هاتفك الذكي كعامل إضافي، من خلال إرسال رمز صالح للاستعمال مرة واحدة في رسالة نصية يجب عليك إدخاله لتتمكن من الدخول لحسابك. وهكذا سيكون على المخترق الوصول إلى هاتفك ورسائلك النصية بعد أن يخترق حسابك المصرفي أو خدمة الوسائط الاجتماعية التي تستخدمها أو كلمة مرور حسابك على وسائل التواصل الاجتماعي، وهذا أمر لن يتمكن منه على الأرجح إذا كنت أنت وهاتفك في نيويورك وكان المخترق في موسكو. وبينما يمثل التحقق المزدوج من الهوية بلا شك خطوة بالاتجاه الصحيح، فإنه يمكن تخريب هذه الأنظمة بهجوم من نوع "الرجل في الوسط" يقوم باعتراض الرسائل النصية عبر برمجيات خبيثة خاصة بالهواتف المحمولة.

لهذه الأسباب تلتفت العديد من شركات الهاتف الذكي مثل آبل

وسامسونغ باتجاه شكلٍ آخر من الأمن المزدوج عبر الدمج بين شيءٍ تعرفه وشيءٍ يمثل هويتك، كالبصمات أو الهوية الصوتيّة. سيزداد استخدام بصماتك كبديلٍ لكلمة السر، ومع الإصدار السادس من آيفون ونظام تشغيل الهاتف الذكي آي.أو.إس 8 سمحت آبل للشركات الأخرى، مثل بايبال والمصارف، باستخدام حسّاس البصمة على هاتفك للتحقق من هويتك. وعلى الرغم من أنّ قراصنة مثل نادي كاؤوس للحاسب قد تمكنوا من مراوغة هذه الأنظمة في السابق (إذا تمكنوا من الوصول إلى الجهاز نفسه)، فإنّ التحقق المتعدد العوامل من الهوية، من شأنه أن يقدمّ تحسيناً كبيراً مقارنةً بالأسلوب التقليدي المعتمد على اسم المستخدم وكلمة السر. فمات هونان على حق، لقد حان الوقت للتخلص من كلمة السر والانتقال إلى التحقق المتعدد العوامل للهوية وإلى الاعتماد على البيانات البيومترية. إذ تمثل تلك الأدوات، وإن كانت أبعد ما تكون عن الكمال، تحسيناً هائلاً إذا ما قورنت بسلاسل الأحرف والأرقام الضعيفة التي نستخدمها اليوم. وعلى الرغم من عدم توفرّ ترياقٍ ناجع حالياً لعملية التحقق من هوية المستخدم، فثمة فرصٌ هائلة لتطوير بدائل أفضل بكثير خصوصاً عبر التنسيق في عمليات البحث والتمويل كما سنناقش في ما يلي.

تعميم التشفير

ثمة نوعان فقط من الشركات، تلك التي تم اختراقها وتلك التي سيتم اختراقها.

روبرت موللر، المدير السابق في مكتب التحقيق الفيدرالي

الغالبية العظمى من بياناتنا اليوم غير مشفرّة وضعيفة الحماية، وقد كشفت دراسةٌ أجرتها عملاق الحاسب إتش.بي في تموز عام 2014 عن أن 90 بالمئة من أجهزتنا المتصلة بشبكة تجمع بياناتٍ شخصيّة يتم مشاركة 70 بالمئة منها عبر الشبكة من دون أي شكل من أشكال التشفير. هذا يعني أن

أي شخصٍ يتمكن من الوصول إلى نظام حاسبٍ معين بسبب برمجياتٍ رديئة أو برمجيات خبيثة يتم تنزيلها أو كلمات سرّ ضعيفة، يستطيع أن يسرق ويقرأ ويستخدم أياً من البيانات المحتواة في هذا النظام. فمن دون تشفيرٍ تكون البيانات قابلةً للقراءة تماماً من قبل أي شخص يتمكن من الوصول إليها، وهو ما مكنّ شبكة الجريمة من استخدام 55 مليون بطاقة ائتمانيّة سرقت من بيانات هوم ديبوت، حيث لم يكن قسم التسديد الداخلي يشفر البيانات الائتمانيّة للمستخدمين. ولو أنّ البيانات قد شفرّت كما ينبغي، لبقيت بلا قيمةٍ بالنسبة للصوص الذين سرقوها. وليست البيانات المالية هي وحدها التي تبقى في معظم الأحيان من دون تشفير، بل ينطبق الأمر أيضاً على السجلات الطبية والأسرار التجارية وقنوات الفيديو العسكريّة الصادرة عن الطيارات المسيرّة وصور المشاهير وهم عراة وجميع رسائل بريدنا الإلكتروني تقريباً. كان من الممكن التخفيف من آثار جميع هذه الاختراقات الحاسوبية وسرقات البيانات إلى حدٍّ كبير لو تم تعميم نظام مناسب للتشفير كسلوكٍ معياري.

تكون معظم البيانات المخزنّة على السواقات الصلبة، سواءٌ كانت عائدةً لأفراد أو شركات، في تنسيقٍ نصّي بسيط يمكن قراءته من قبل أي شخص يصل إلى هذه الأجهزة. وهو ما ينطبق أيضاً على جُلِّ البيانات التي تنتقل من مكانٍ إلى آخر عبر الإنترنت، في ما عدا مواقع الويب الكبرى التي تستخدم بروتوكل النقر المشفر إتش.تي.تي.بي.إس. عند إرسال كلمات سرّك أو معلومات بطاقتك الائتمانيّة. لكنّ بإمكاننا أن نحسن الوضع القائم إلى حدٍّ كبير، تحديداً مع الصحوة التي تسببت بها تسريبات إدوارد سنودن. فعلى الجانب المضيء تستخدم، غوغل التشفير على نحوٍ متزايد في البيانات التي تنقلها بين حاسبك ومخدماتها (لا فقط كلمة سرّك)، بما فيها جميع رسائل جيميل. وهي بذلك تجعل من الصعوبة بمكان علي أيّ شخصٍ أن

يعترض ويقرأ رسائل بريدك الإلكتروني أثناء نقلها. فمن دون ذلك التشفير تكون أية رسالة ترسلها أشبه ببطاقة بريدية يمكن الوصول إليها بسهولة من قبل أي شخص يرى المحتويات وهي تتنقل عبر أنحاء الإنترنت، عبر اتصال الوايفاي المحلي الذي تستخدمه في مقهى ستار باكس على سبيل المثال. وقد أطلقت منظمة الحدود الإلكترونية، وهي مجموعةٌ غير ربحية تدافع عن الحقوق الرقميّة وعن الخصوصيّة، برنامجاً يعرف باسم "اتش.تي.تي.بي.إس في كل مكان" للترويج لاستخدام التشفير في جميع عميات تبادل المعلومات التي تجري بواسطة متصفح الإنترنت. باختصار، لقد حان الوقت لتشفير الإنترنت دعماً لخصوصيّة اتصالاتنا الرقمية وبياناتنا الحاسوبية وأمنها.

على الرغم من أن أنظمة تشغيل الحاسب الحديثة، بما فيها أنظمة مايكروسوفت وآبل، تأتي مع أدوات تشفير مجانية للقرص الصلب، فإنّ هذه الأدوات ليست مفعلةً تلقائياً، وقلةٌ قليلة من الشركات ونسبةٌ لا تذكر من المستخدمين تشفّران البيانات على حواسبهما المحمولة أو المكتبية. بل إنّ معظم المستخدمين لا يعلمون حتى بوجود بروتوكولات الأمن هذه. في أعقاب كبوة الاختراق الذي طال خدمة أي كلاود للمشاهير عام 2014، اعترف كبير مديري آبل كيم كوك بأن على الشركة أن تقوم بمزيدٍ من الجهد لزيادة وعي المستهلكين بقضايا الأمن السايبري. وهو ما أوافق عليه تماماً. ففي أيلول عام 2014 أعلنت آبل أنّ جهاز الآيفون التالي سوف يشفر جميع البيانات على الجهاز حين يتم وضع كلمة مرور، في حركةٍ تعهّدت غوغل بمجاراتها في نظام تشغيلها للهاتف النقال أندرويد في إصداره القادم. وهي خطواتٌ هامة في الاتجاه الصحيح نحو خفض المخاطر الأمنيّة للهاتف الذكي، لكن إذا بقي 40 بالمئة من المستخدمين لا يستخدمون حتى كلمة مرور على هواتفهم النقالة فإنّ تيم كوك على حق: لا بد من مزيدٍ من التوجيه

والتوعيّة.

تجنّب بعض الجريمة السايبرية: لا بد من التعليم

الحضارة في سباق بين التعليم والكارثة.

إتش. جي. وِيلز

لدينا مشكلة أمية في الولايات المتحدة وفي أنحاء العالم تختلف عما يتصوره معظمنا، فهي مشكلة الأمية التقنيّة. ففي عالمٍ يعجّ بالأدوات والخوارزميات والحواسب والأجهزة القابلة للارتداء وشرائح المعرّفات الترددّيّة الراديوية والهواتف الذكية، لا تتوفر سوى لقلةٍ قليلة من السكان فكرةٌ عن الطبيعة الفعلية لعمل هذه الأغراض. وسواءٌ كانت شركة الجريمة أم وكالة الأمن القومي، فإنّ أولئك الذين يعرفون كيف تكتب الشيفرات الحاسوبية سيحتفظون بسلطتهم المتفوقّة على أولئك الذين لا يعلمون، بالطريقة نفسها التي كان فيها أولئك الذين لا يعرفون القراءة والكتابة في القرون السابقة يجدون الإمكانات المتاحة أمامهم محدودة. لذا فإنّ علينا أن نمحو الأميّة التقنيّة لدى الجماهير.

ليس الهدف هو أن يصبح كل شخصٍ مبرمجاً (ولو أنّ بناء مهارات العلم والتقانة والهندسة والرياضيات في البلاد سيقدم الكثير لاقتصادنا). بل الهدف هو أن يتكون لدى المواطنين فهمٌ أساسي لطرق عمل التقانات التي تحيط بهم، لا فقط أن يستخدموا هذه الأدوات ويستغلوها استغلالاً كاملاً، فمن الهام أيضاً ألا يستغل آخرون الجهل التقاني لإلحاق الأذى بالغير. فلو تمّ تعليم كاسيدي وولف، ملكة جمال المراهقين في الولايات المتحدة، الحيلة البسيطة التي تقوم على تغطية كاميرا الويب على الحاسب المحمول بلصاقة ملاحظاتٍ صفراء، لما أمكن للقرصان أبداً أن يلتقط صوراً لها سرًّا وهي عاريةٌ في غرفة نومها. وما هذا بالطبع سوى مثال واحد، ففي حالة تلو الأخرى من حالات الهجمات السايبرية، يتبين دائماً أنه لو كانت الضحية

مسلحةً ببعض المعرفة الصحيحة حول كيفية حماية نفسها، لأمكن تجنب آلام الاختراق برمتها. فالتعليم هو المفتاح، وحالة الثقافة الأمنيّة - السايبرية لدينا مزريّة.

نؤمن لأطفالنا في مدارسنا العامة كلّ شيء من الثقافة الجنسيّة إلى التعليم على القيادة. لكن أطفالك سيمضون من الوقت على الإنترنت وفي التفاعل مع التقانة أكثر بكثير مما سيمضون في الجنس والقيادة على الأرجح. إلا أنّ معظم المدارس لا تقدم سوى قدرٍ ضئيل من التعليم الرسمي حول كيفية البقاء في مأمنٍ على الشبكة. وقد دأُبَ ماك.غراف من المجلس الوطني للوقاية من الجريمة على مدى سنوات، من خلال برنامجه "كرايم دوغ"، على تحذير الأطفال والبالغين على حدٍّ سواء عبر التلفاز وفي المدارس من "تجنب بعض الجريمة". ونحن اليوم بأمس الحاجة إلى ماك.غراف، وأكثر من أي وقتٍ مضى، ليعلم أبناءنا كيفية تفادي بعضٍ من الجريمة السايبرية. وثمة لحسن الحظ بعض التجارب المفيدة التي يجري العمل عليها. فقد أطلق المجلس الوطني للوقاية من الجريمة عدة برامج لتوعية الأهالي والأطفال من التنمّر السايبري وطرق تحقيق السلامة عبر الإنترنت. كما أنشأ التحالف الوطني للأمن السايبري موقع ويب ممتازاً (StaySafeOnline.org) والعديد من البرامج الشعبيّة الأخرى للمساعدة في توعية مجتمعنا الرقمي إلى استخدام الإنترنت بطريقةٍ آمنة، سواءٌ من البيت أو من العمل أو في المدرسة. لكن لا بدّ من توسيع هذه التجارب توسيعاً كبيراً إذا أردنا أن نواجه مستوى التهديد الذي يقف في طريقنا عبر طيفٍ واسع من التطورات التقانية مثل إنترنت الأشياء. وكما نوهنا سابقاً، فإن معظم هذه التهديدات التقانية لا بد من مجابتها والتعامل معها على مستوى النظام، لكن على الأفراد أيضاً أن يدركوا المخاطر القائمة وأن يتحملوا مسؤولية حماية أنفسهم وعائلاتهم قدر المستطاع. ونحن بحاجةٍ،

بهذا القدر نفسه، إلى التوعية بين الشركات في القطاع الخاص. فالشركات عرضةٌ للهجوم، لا فقط من قبل شركة الجريمة، بل أيضاً من قبل أجهزة التجسس الحكوميّة المعقدّة التي تسعى وراء الملكية الفكرية والبيانات التجارية. فالإجراءات الأمنيّة التي كانت عادةً ضروريةً في كبرى المنظمات السريّة، باتت اليوم ضروريةً للغاية في عالم الأعمال بأسره. وهنا أيضاً نجد أنّ الموارد التعليمية محدودةٌ للغاية وهي حالة سائدة لا بد من معالجتها إذا أردنا أن نحقق أي تقدم في كفاحنا ضد التهديدات التقانية التي ترتسم في أفقنا.

العامل البشري: الحلقة الأضعف المنسيّة

> إذا كنت تعتقد أن التقانة تستطيع حل مشكلاتك الأمنيّة فإنك لا تفهم المشكلات ولا تفهم التقانة.
>
> بروس شناير

ليس الأمن السايبري مشكلةً تقنيةً وحسب، بل هي مشكلة الناس أيضاً. فمهما كانت كلمة مرورك على الحاسب قويّة، فإنك إذا دونتها على لصاقةٍ صفراء تضعها أمام شاشة حاسبك لكي تتذكرها، سيتمكن أي شخص يمرّ بجوارك من الوصول إلى حياتك الرقميّة. وعشرات الآلاف من الناس الذين يخسرون أموالهم بسبب رسائل البريد الإلكترونية الاحتيالية النيجرية كل عام، ليست مشكلتهم مشكلةً تقانية، بل هي مشكلة الخصال البشرية الأبديّة من الأمل والطمع. وعندما تنشر خطط إجازتك على الوسائط الاجتماعيّة ويمرّ اللصوص لزيارة منزلك في غيابك، فقد كان القرار قرارك عندما شاركت معلوماتٍ ساعدت النشاط الإجرامي. وجميع أولئك الذين ينقرون على رابطٍ يأتيهم من مصرفهم ويقول لهم إن كلمة مرورهم قد انتهت صلاحيتها وصار يجب تغييرها، لا يمكن التحدي في كون حواسبهم قد تعرضت للاختراق فقط، بل إنها بالأحرى مشكلتهم هم الذين وقعوا ضحيةً

لهجوم تصّيد يعتمد على الهندسة الاجتماعية. ومهما كان عدد الجدران النارية وتقانات التشفير وبرمجيات مكافحة الفيروسات التي تستخدمها شركةٌ ما، فإنّ وقوع الكائن البشري الذي يجلس خلف لوحة المفاتيح في فخٍ ما سيكفي للقضاء على الشركة. ووفقاً لدراسةٍ معمّقة أجرتها خدمات الأمن في آي.بي.إم عام 2014، فإنّ 95 بالمئة من الحوادث الأمنيّة كانت تشتمل على خطأ بشري. فمن شأن العامل البشري أن يُبطل مفعول جميع الإجراءات الأمنيّة التقانيّة الأخرى، لذا لا بد من توعية الكوادر العاملة والأفراد على حدٍّ سواء.

كما ذكرنا في المقدمة، تستطيع التقانة بالطبع أن تساعدنا على زيادة مستوى أمننا. فمن شأن التحقق المتعدد العوامل من الهويّة وتوظيف البيانات البيومترية والتشفير ومراعاة الموقع الجغرافي، أن تحسُر الجريمة وتخفّض غيرها من الأخطار الأمنيّة. لكن كما رأينا مراراً، ربما يُستهان بقدرة هذه الأدوات التقانية. فلا شك بأنّ وكالة الأمن القومي تمتاز بأحدث أدوات الأمن السايبري تحت تصرفها، إلا أنّ بشرياً هو إدوارد سنودين هو الذي خربها حين هرب ببياناتٍ سرّية حساسة على قرصه المحمول. والأمر نفسه يصحّ على منشأة الطاقة النووية "السلميّة" في ناتانز، التي كانت تطبق إجراءاتٍ أمنية جيدة ولم تكن تقيم اتصالاً بين نظم التحكم الصناعي لديها والإنترنت الواسع. إلا أنّه كان من السهل تجاوز كل هذه الإجراءات عندما عثر مهندسٌ إيراني على قرصٍ محمول في ساحة مواقف السيارات التابعة للمنشأة فأخذها ووضعها بلا مبالاة في حاسبٍ مكتبي. وسمح هذا القرار الذي ينّم عن جهل لدودة ستاكس نت بالانتشار عبر الشبكة الداخلية المسؤولة عن التحكم بأجهزة طرد اليورانيوم في المنشأة. من المريح اللجوء دوماً إلى حلٍ تقاني سهل للمشكلة، لكن لا بد من أصحاب الأعمال وواضعي السياسات وشركات الإنترنت ومبرمجي الحاسب والمهندسين من أخذ البعد

البشري للأمن في اعتبارهم، إذا ما أردنا أن نُحرز أي تقدمٍ ضد المخاطر التقانية التي تواجهنا اليوم وستواجهنا غداً.

الخبر الجيد هنا هو أنه بوسعنا فعل الكثير عبر تكييف سلوكنا البشري لتحسين الأمن التقاني الشخصي تحسيناً كبيراً. ولكي نضع هذا الجانب في إطاره الصحيح، من المفيد أن نفكر في سرقة السيارات على سبيل المقارنة. فحين يركنُ مالك سيارة بي.إم.دبليو سيارته في حيّ يعجّ بالجريمة، فإن القرارات التي يتخذها شخصياً حول أمن السيارة سيكون لها أثرٌ كبير على احتمال سرقتها. فحين يركن السائق في منطقة جيدة الإضاءة ويقفل جميع الأبواب والنوافذ ويشغل جهاز الإنذار، يكون قد اتخذ جميع الإجراءات المناسبة لمنع اللصوص من سرقة سيارته. لقد تعلم معظمنا مع الوقت أن هذه هي الطريقة الصحيحة لتأمين مركباتنا، لكن غالبية الناس ليست لديهم أية فكرة عن السلوك المناسب في الفضاء السايبري، لذا فإننا نبحر في الإنترنت ونركن سياراتنا افتراضياً في طرقاتٍ معزولة ومظلمة ونترك الأبواب والنوافذ مفتوحة ولا نستخدم جهاز الإنذار قط وننسى المفاتيح داخل السيارة، ونترك أوراقاً نقديّة من فئة المئة دولار على المقعد الأمامي. ثم نتعّجب حين تتعرض سيارتنا للسرقة.

ليس الهدف هنا هو الوصل إلى ما يشبه حصاناً أحادي القرن وهمياً هو "الأمن المطلق"، بل إحراز تحسين ملحوظ على الوضع القائم. ولنا هنا أن نعود إلى مثال السيارة أعلاه. فحتى حين يتخذ السائق جميع الخطوات والإجراءات الوقائيّة لحماية نفسه وحماية سيارته، فإنّ سرقة العربة قد تقع مع ذلك. فقد يأتي مجرمٌ مع عربةٍ مسطحة أو شاحنة قطر، ناهيك بأن يخلع الأبواب والمحرك ويهرب بالعربة. حين يتوفر ما يكفي من الوقت والطاقة والانتباه والموارد، يمكن اختراق أي نظام. فالهدف هو ليس الأمن المطلق، بل الهدف هو فهم كيف تقفل أبواب ونوافذ سيارتك في الفضاء

السايبري، وفي إدراك أنّ الكثير يمكن التحكم به. مع ذلك، فإنّ الكثير من القرارات المحفوفة بالمخاطر التي تتخذ على الشبكة اليوم ليست خطأك بالكامل بل إنها ناتجة عن نظم حاسوبية ومواقع ويب وهواتف ذكية وبرمجيات وتجهيزات رديئة التصميم إلى حدٍّ لا يعقل. وقد حان الوقت لإصلاح كل ذلك.

تطبيق التصميم الموجه للمستخدم في المجال الأمني

> تبدأ الفرص الجديدة للابتكار عندما تبدأ عملية حل المشكلات الإبداعيّة متعاطفاً مع جمهورك الذي تخاطبه.
>
> توم كيلي، من إيديو

ما بال هؤلاء المستهلكين الحمقى لا يحدثّون كلمات مرورهم؟ لو أنّ هؤلاء الأغبياء يستخدمون الشبكات الخاصة الافتراضية والجدران النارية فقط. حسناً، وهل تستخدم أنت الخصوصيّة المكافئة للشبكات السلكية (دبليو.إي.دي) أو معيار الوصول المحمي للشبكات اللاسلكيّة بإصداره الثاني؟

كما يعلم كل شخصٍ اتصل بالدعم الفني ليحلّ مشكلةً مع الحاسب، فإنّ معظم مديري الأنظمة وكوادر الدعم الفني لا يولون "زبائنهم" كبير شأن. فالتشخيص الأكثر شيوعاً بين كوادر الدعم التقني هذه يختصر بكلمة بيكنيك، الاختزال الإنكليزي لعبارة "المشكلة في من يجلس على الكرسي لا في الحاسب". فبالنسبة لمن درسوا علم الحاسب وأخذوا دروساً في التشفير ورأوا أحلاماً بلغة بي.إتش.بي وسي++ فإنّ الحديث مع مستخدم حاسبٍ متوسط قد يكون عمليةً محبطة. فنحن نتكلم لغتين مختلفتين بكل معنى الكلمة. فبالنسبة لمهندسي الأمن، يبدو الجواب واضحاً كما يلي: "لو أنّ هؤلاء المستخدمين الملاعين يكفّون عن القيام بـ س أو ع من الأشياء الغبيّة لكان كل شيء على ما يرام". أما المستخدمون على الطرف الآخر من الخط

فلديهم طلبٌ بسيط غالباً ما لا يعبرون عنه: "لماذا لا تعطني بعض التعليمات البسيطة وتسمح لي بالعودة إلى عملي؟" فالأدوات الأمنية المتوفرة لدينا اليوم أعقد وأصعب من أن يتم استخدامها، كما أنّ التعقيد، إذا أردنا التبسيط، هو عدو الأمن.

يتحدث مهندسو الأمن المعلوماتي باستخدام عباراتهم التخصصيّة عن الفيروسات والبرمجيات الخبيثة وهجومات اليوم صفر، والثغرات البرمجية وأحصنة طروادة وفيروسات التحكم عن بعد ومعايير التشفير المتقدمة، لكن معظم العامة لا يمتلكون أية فكرةٍ عما يتحدث عنه هؤلاء المهندسون. فالمنتجات الأمنيّة البرمجية والعتادية اليوم تكاد كلها تكون مبنية من قبل محترفين من أجل المحترفين. أما كيف ستستخدم هذه الأدوات من قبلك، ناهيك بجدّتك، فهو أمرٌ قلما ينال بعض التفكير أو التعاطف. وبدلاً من ذلك، تطلع علينا هذه المنتجات التي يفترض بها أن تحمينا وتقدم لنا الأمن بتحذيراتٍ من قبيل "تحذير: عملية مُضيفة لأحد خدمات ويندوز تستخدم بروتوكول يو.دي.بي الخارج ورقم عبور بروتوكول الإنترنت من الإصدار السادس، تحاول الاتصال بالإنترنت. هل تود المتابعة؟" فماذا يعني ذلك بحق الجحيم؟ ما من أحدٍ يعلم سوى المصممين الأصليين لهذا التحذير "المفيد". لقد آن الأوان لتطبيق التصميم الموجه للمستخدم وطرق تفكيره في عالم الأمن السايبري.

فكر بتصميم هاتف الآيفون 6 أو بأريكة إيمز، أو بسيارة فيراري 458 إيطاليا، أو كاميرا ليزاتي، تلك المنتجات التي تهدف إلى إبهاج من يشتريها. فهذه الأدوات ليست فقط ناجحة في أداء عملها، بل هي جميلةٌ أيضاً، صنعها أشخاصٌ يدركون عن كثب وبعمق ماهية زبائنهم وحاجاتهم. حين كان المرء يشاهد ستيف جوبز على المنصّة يصف آخر منتجاته، ما من شكٍ في أنه سيتشبع حباً بصانعي هذه المنتجات. فأين ستيف جوبز في مجال

الأمن؟ وماذا يمكن لكبير مصممي آبل، جوني إيف، أن يقدم لمشكلة انعدام الأمن السايبري المتنامية؟ وكيف سيبدو جدار النار أو برنامج مكافحة الفيروسات لو كان من تصميمه؟ ما من فكرةٍ لدينا حتى الآن، وهذه مشكلةٌ كبيرة.

إنها مشكلةٌ لأنه حين تكون الميزات الأمنيّة سيئة التصميم، فإن الناس ببساطة لا يستخدمونها. علاوةً على ذلك، فإنّ التصميم الرديء قد يدفع المستخدمين البشر لاتباع طرقٍ تجعلهم أقل أماناً في الواقع. فلماذا يدوّن الناس كلمات مرورهم على لصاقاتٍ ويضعونها أمام حواسبهم؟ لأن إرغام الناس على تغيير كلمة مرورهم كل أسبوعين واشتراط أن تحتوي الكلمة على عشرين حرف على الأقل بينها حروفٌ كبيرة وصغيرة ورقم ورمز وبيت من الهايكو وقصيدةٌ خماسيّة، هو ببساطة أمرٌ مبالغٌ فيه لا يمكن للمستخدم العادي أن يتعامل معه. وهو ما يدفع الناس إلى تخريب النظم الأمنيّة قيد العمل لكي ينجزوا مهامهم. وثمة أيضاً أنواعٌ من المنتجات الأمنيّة، كجدران النار البرمجيّة، تطلق من الإنذارات الكاذبة ما يدفع الشخص الذي يشغل هذه الأدوات إلى إيقافها تجنباً لرسائل التحذير غير المفهومة التي تنبثق طوال الوقت. في هذه الحالات، عندما تقع اختراقاتٌ أمنيّة، دائماً ما تنحى كوادر تقانة المعلومات باللوم على المستخدم. فربما حان الوقت للنظر في المرآة أولاً. ليس مصممو المنتجات الأمنيّة والأنظمة أشخاصاً لا مبالين أو جهلة، بل كل ما في الأمر هو أنهم بعيدون عن التّماس مع حاجات زبائنهم على نحوٍ بائس. إذا أردنا استعارة عبارةٍ، فقد حان وقت "التفكير بشكل مختلف".

تصميم المنتجات الموجه للمستخدم هو مكوّن أساسي لا بد منه لفرض التغييرات السلوكية التي نحتاج إليها في عالم الأمن التقاني، وللمساعدة على تخفيف العدد المتنامي من التهديدات التي نواجهها. ويحتاج مصممو هذه

المنتجات إلى فهمِ طريقة تفاعل الناس مع الحواسب والهواتف الذكية على مستوى جيد، وعليهم ألا يتوقعوا من الناس أن يلتزموا بسلوكٍ غريب أو أن يفهموا الرسائل الغامضة التي تظهر لهم على الشاشة. وإلى أن يبدأ محترفو الأمن بتصنيع منتجاتٍ تستطيع الجماهير الأعرض فهمهما وتطبيقها، سيبقى الناس في عوزٍ إلى الأدوات والمعلومات التي يحتاجون إليها لحماية أنفسهم. فيما ما من شكٍ في أنّ البرامج التوعوية والتصميم الموجه للإنسان من شأنها أن تحقق تحسناً كبيراً على الحالة العامة السائدة في مجال الأمن التقني اليوم، فإنّ بعض التهديدات تتجاوز قدرة فردٍ منعزل. ففي هذه الحالات يكون لا بد من مجموعةٍ من التغييرات التي تطال النظام، ويمكن استلهام أفضل طريقٍ نمضي بها من الطبيعة والطب.

أمُنا (الطبيعة) هي أفضل من يعلم: بناء نظام مناعة للإنترنت

تتجاوز التهديدات السايبرية في سرعة تطورها قدرة أسوارنا الدفاعيّة على إبقائها في الخارج، فالأعداء البرابرة ليسوا فقط على البوابة، بل اقتحموها، وها هم يزحفون في كل مكانٍ في القلعة. نحن بحاجةٍ إلى وسائل دفاعيّة أكثر متانةً وأسرع استجابةً وأكثر مرونةً، أشبه ما تكون بالنظام المناعي في الجسم. فخلال أكثر من ثلاثة مليارات عام وُجدت خلالها الحياة على هذا الكوكب، تعلم الملايين من الأنواع المختلفة، ومن بينها الكائنات البشرية، كيف تتعامل مع هذا الطيف الذي لا ينتهي من التهديدات. وما يؤمن الحماية لدى الحيوانات هو نظام مناعتها القادر على التكيّف، والذي يقف في وجه طيفٍ واسع من مسببات المرض الغريبة، منها الفيروسات والطفيليات والباكتيريا بل حتى السموم البيئية. من شأن التصاميم التي نراها في كل مكانٍ حولنا في الطبيعة أن تكون مصدر إلهامٍ عظيماً لنا في سعينا لحل مشكلات البشر المعقدة، وثمة مجال بحثي مخصص لهذا التحدي يدعى المحاكاة البيولوجية. إذ يعكف العلماء اليوم على سبيل

المثال على دراسة كيفية معالجة أوراق النباتات للطاقة الشمسية، بهدف التوصل إلى ألواح شمسية أفضل. فلمَ لا نلجأ إلى الابتكار المستوحى من الطبيعة، علّه يساعدنا على خلق شبكاتٍ حاسوبية تعالج نفسها بنفسها.

اعتمدنا حتى الآن في معالجتنا لمسألة الأمن السايبري على تسوير أنفسنا تجنباً لجميع التهديدات التقانية المحتملة، لكن عدم استخدام الإنترنت أو التقانة ليس خياراً. فثمة أسلوبٌ أفضل بكثير يقوم على الاعتراف بالمخاطر والتأقلم معها بسرعة حين تبرز، تماماً كما تفعل أنظمتنا المناعيّة. فالنظام المناعي البشري ليس ناجعاً بوجه سلالةٍ بعينها من الإنفلونزا، بل هو يتأقلم بسرعةٍ ويتعلم كيف يتعامل مع طيفٍ واسع من سلالات الإنفلونزا. وهو أمرٌ ممكن بفضل الحسّ الثاقب الذي يتوفر في جسدنا لفهم ما يشكل "الذات الصحيّة" وتمييزها عن "الغير" الخطير. لكن مثل هذه الطرائق لا تزال بدائيةً في أحسن أحوالها لدى نظم الدفاع التقاني الموجودة لدينا اليوم. وقد أطلقت كل من إدارة مشاريع الدفاع داربا والمخبر الوطني لشمال غرب المحيط الهادي مشاريع تتناول هذا الموضوع، وقد بدأ يتبدّى بالفعل حلٌ في غاية الإثارة في جامعة ويك فوريست. حيث يقوم الأستاذ في علم الحاسب هناك إرين فَلب باستخدام ذكاء الأسراب الطبيعي المتوفر في مستعمرات الحشرات لصدّ الحيوانات المفترسة السايبرية، عبر نشر الآلاف من "النملات الرقميّة" البرمجيّة عبر شبكة الحاسب، لتقوم كلٌّ منها بالبحث عن دليلٍ على وجود خطر. وإذا ما اكتُشف مثل هذا التهديد، تقوم النملة الرقميّة بترك إشارةٍ أشبه بالعطر الافتراضي الذي يجتذب النملات الأخريات. وكلما ازدادت قوة العطر، ازداد عدد النملات الرقميات التي يجذبها، ما يتكفّل بمحاصرة أي عدوى حاسوبية محتملة في النهاية قبل أن تخرج عن السيطرة. تبلغ معدلات توسّع الهجمات السايبرية حدوداً يستحيل على الكائنات البشرية مواكبتها يدوياً. وبالمثل فإنّ هدفنا يجب أن ينصبّ على

تطوير مجموعةٍ من الحسّاسّات التي ننشرها على شبكاتنا العامة، لا فقط لاكتشاف أمر الدخلاء وكيف أمكنهم الدخول فحسب، بل، وهو الأهم، إجراء الإصلاحات الضرورية آلياً بما يخلق شبكةً قادرة على شفاء نفسها ولا تتطلب تدخل الإنسان لإصلاحها. إنّه نظامٌ مناعي للكوكب. وإلى أن يبدأ مثل هذا النظام بالعمل، سنستمر بتركيز جهودنا على طرائق تحتاج إلى استثمار رأس مالٍ بشري كبير لحل المشكلة كاللجوء إلى السلطة التنفيذية للقبض على المجرمين.

خفر القرن الحادي والعشرين

> في عالمٍ يسوده التغيير المدفوع بالتقانة، ليس أمامنا سوى أن نشرّع بعد أن يقع ما يقع، أي إننا نزحف زحفاً طوال الوقت لكي نواكب ما يجري.
> وليام جبسون

ليس خفرُ الشبكة مسألةً بسيطة. ونحن نسمع بالتأكيد قصصاً عن وكالة الأمن القومي، القادرة على أي شيء على ما يُزعم وهي تتبع كل حركةٍ لنا في الفضاء السايبري، فلا شكّ في أنها تمكنت من تجميع ترسانةٍ فعالة من الأدوات والتقنيات. لكن الإنترنت تبقى بالنسبة لضابط الشرطة أو المحقق العادي مكاناً يصعب العمل فيه. فرجال الشرطة في الشعبة 77 في قسم شرطة لوس أنجلوس، أو في دائرة وسط المدينة الجنوبي في قسم شرطة نيويورك أو في قسم شرطة إنغلوود في لوس أنجلوس، لا تتوفر لديهم أي من هذه الأدوات التي تستخدمها وكالات التجسس، فهي جميعها أدوات سرّية وأكثر حساسية بكثير من أن يتم تقديمها في محكمة. بل إن منظمات مثل مكتب التحقيقات الفيدرالية، تواجه حواجز لا يستهان بها خلال إجرائها للتحقيقات في الجريمة السايبرية خصوصاً في ما وراء البحار. فعلى مستوى الولاية وعلى المستوى المحلي والفيدرالي، تجد السلطة التنفيذية نفسها

مغلوبةً على نحوٍ مزمن تنقصها الكوادر، كما يشهدُ النمو الانفجاري في الجريمة الشبكيّة الذي فصّلناه في صفحات هذا الكتاب. كما تبين الخسائر السنويّة للاقتصاد العالمي، والتي تقدر بـ400 مليار دولار ناتجة عن الجريمة السايبرية، الخسارة الفادحة للشرطة في حربها ضد شركة الجريمة.

عادةً ما يستفيد المهاجمون، تدفعهم الأرباح التي يحققوها عبر مغامراتهم في الأوساط السريّة الرقميّة، من التقانة بشكلٍ عام قبل المدافعين والمحققين بوقتٍ طويل. إذ تتوفر لديهم ميزانياتٌ تكاد تكون غير محدودة، وليس عليهم التعامل مع بيروقراطيات داخليّة وعلميات موافقة وقيود قانونية. لكن ثمة مسائل أخرى تتعلق بالنظام تمنح المجرمين اليد العليا، خصوصاً تلك المتعلقة بالمناطق القانونية والقانون الدولي. ففي غضون بضع دقائق، يمكن للمجرمين أن يزوروا افتراضياً ستة بلدانٍ مختلفة، متنقلين من مخدمٍ إلى آخر ومن قارةٍ إلى أخرى في لمح البصر. فماذا عن الشرطة التي يترتب عليها تتبع آثر الأدلة الرقميّة للتحقيق في القضية؟ ليس هناك الكثير، فكما في جميع النشاطات الحكومية الأخرى، لا بدّ من اتباع السياسات والإجراءات والتشريعات. وتفرض الهجمات السايبرية العابرة للحدود إشكالاتٍ جديّة تتعلق بمناطق النفوذ القانونية، لا فقط بالنسبة إلى قسم شرطة بعينه، بل لمؤسسة الشرطة برمتها في صيغتها الحالية. إذ لا يمتاز شرطيٌّ في دالاس بسلطةٍ تخولّه إرغام مزود خدمة إنترنت في طوكيو على تقديم دليلٍ ما ولا يمكنه أن يلقي القبض على أحدٍ في منطقة غينزا. ولا يمكن إنجاز ذلك سوى عبر طلبٍ بين الحكومتين غالباً ما يعتمد على اتفاقيات مساعدة قانونية متبادلة. والوتيرة البطيئة إلى حد الكارثة للقانون الدولي عادةً ما تجعل الحصول على دليلٍ مما وراء البحر يتطلب سنواتٍ (في عالمٍ يمكن فيه تدمير الدليل الرقمي خلال ثوانٍ). والأسوأ من ذلك هو أن غالبية البلدان لا تتوفر لديها حتى الآن قوانين لمكافحة الجريمة

السايبرية وإن على الورق، ما يعني أن المجرمين يتصرفون متمتعين بالحصانة. وكما رأينا من حال تجار المخدرات وغاسلي الأموال، يبقى المجرمون السايبريون بحكمة في بلدان المرافئ الآمنة.

يعتبر القانون الجنائي مسألةً قومية بهدف احترام سيادة كل بلد على قوانينه وتشريعاته دون تدخل خارجي في أموره الداخلية، ويعود تاريخه إلى معاهدة فيستفاليا عام 1648، ومع أن نظاماً كهذا بقي يعمل على نحوٍ جيد على مدى قرون، فإنّه اليوم يخضع لضغطٍ متنامٍ بلا هوادة من الإنترنت العالميّ الذي يحث مثل هذه الحدود. والإبقاء على اتفاقية فيستفاليا هو جوابٌ جغرافي لمشكلة غير جغرافية. فالتهديد التقاني الذي نواجهه اليوم لا يعرف الحدود، لذا فإنه لا يمكن التعامل معه سوى عبر استجابةٍ دولية مناسبة. وثمة دورٌ هام يمكن للإنتربول، منظمة الشرطة الجنائيّة الدولية، أن يؤديه في مكافحة الجريمة السايبرية العابرة للقوميات، عبر التنسيق بين التحقيقات التي تجريها 190 دولة عضواً. إلا أنّه لا تتوفر للإنتربول سوى ميزانية تشغيل قدرها 90 مليون دولار لمكافحة جميع الجرائم الدولية، من الإتجار بالبشر إلى سرقة الفن. للمقارنة، تبلغ ميزانية قسم شرطة نيويورك لوحدها 4.9 مليارات دولار، كما كان في حوزة زعيم عصابات المخدرات يواكين "الشابو" غوزمان لويرا المكسيكي نحو 200 مليون دولار في منزله حين ألقي القبض عليه (أي ضعف ميزانية الإنتربول السنوية ويزيد). فالتحقيقات الجنائيّة، خصوصاً منها تلك التي تشمل مناطق قانونية مختلفة وكميات هائلة من الأدلة الإلكترونية، ليست فقط بحاجة إلى الكثير من العمل، بل لها كلفةٌ استثنائيّة أيضاً. ومن دون زيادة ميزانيات الشرطة لأضعافٍ مضاعفة لحل المشكلة، علينا أن نتوقع تنامي شركة الجريمة من دون رادع لمساعيها غير الشرعيّة.

لكن حتى زيادة موارد السلطة التنفيذية زيادة كبيرة لن تحل مشكلة

التهديدات السايبرية التي نواجهها، فثمة مكونٌ ثقافي في نظامنا القانوني الجنائي لا بد من معالجته أيضاً. ففي عام 2012 اعترفت جانيت نابوليتانو، سكرتيرة وزارة الداخلية في ذلك الوقت، أنها لا تستخدم البريد الإلكتروني أو أية خدمات شبكيّة أخرى "على الإطلاق". أجل، إن المسؤول الحكومي الأرفع الذي يتولى رسمياً مهمة الأمن السايبري للبلاد وحماية البنية التحتية الحساسة لم يكن يستخدم البريد الإلكتروني، ليس بسبب المشكلات الأمنيّة بل لأنها، وفقاً لاعترافها بالذات، "أميل إلى أن أكون من محطمي الآلات". وفي عام 2013 اعترفت قاضية المحكمة العليا الأميركية إلينا غاغان، بأن زميلاتها من القاضيات "لسن أعرف الناس بالتقانة" وأنّ "الحكومة بالفعل لم تصل حتى إلى البريد الإلكتروني بعد". وعوضاً عن ذلك، كما تقول، فإنهم يتواصلون بعضهم مع بعض بواسطة مذكراتٍ يكتبونها على ورقٍ عاجي، وتُحمل باليد من غرفةٍ إلى غرفة في المحكمة من قبل موظفي المحكمة. ومع أنّه ما من مجالٍ للشك في القدرات الفكرية الكبيرة للقاضيات وسكرتيرات الوزارة في قمة نظامنا القضائي الجنائي، فإن النقض الواضح في الاهتمام حتى بأكثر التقانات بدائيةً أو في القدرة على استخدامها جديرٌ بالتنويه. ففي عالمٍ يتحرك بالسرعة التي يتحرك بها عالمنا، كيف يمكن أن توضع سياسة الأمن السايبري الحكومية وقوانين التقانة والخصوصية على يد أولئك الذين لا يستخدمون البريد الإلكتروني؟

ممارسة التقنيات الآمنة: الحاجة إلى نظافة شخصيّة سايبرية جيدة

كلنا يعلم ماذا تعني النظافة الشخصيّة الجيدة في العالم المادي، إذ يتم التأكيد عليها في كل مكانٍ حولنا. وثمة لافتاتٌ في حمامات المطاعم تذكر العاملين بأنّ عليهم أن يغسلوا أيديهم قبل أن يعودوا إلى عملهم. وتخبرك أمُك بأنّ عليك أن تغطي فمك حين تعطس، بينما يذكرك الزملاء والأطباء واللوحات الإعلانيّة بأن عليك استخدام الواقي قبل أن تمارس الجنس الآمن.

لكن أين هذه الرسائل في العالم الافتراضي؟ فما من أمٍ تذكرك بتجنب استخدام إصبع تخزين يأتيك من غريب، لذا فقد اعتدنا إدخال الأجهزة الحاملة للفيروسات في حواسبنا مشاركين من غير علمنا في نشر البرمجيات الخبيثة التي تصيب في النهاية جيراننا وأصدقاءنا. ومن شأن فشلي في اتباع الممارسات الصحيحة جعلي عبداً للقوى الإجرامية يشارك من دون علمه في هجمات حجب خدمة وهجمات تصّيد.

تمثل صحة الإنترنت، على غرار الصحة العامة، مسؤوليةً مشتركة. وعلى المستخدمين أن يتولوا إدارة شبكاتهم وأجهزتهم إذا أردنا أن نرفع من مستوى الأمان في مستقبلنا التقني، وثمة وازعٌ أخلاقي يلزمنا بذلك. فعلى كلٍ منا أن يكون راعياً جيداً على قطيعنا التقاني عبر حماية حواسبنا وهواتفنا ومعداتنا الرقميّة ومنعها من إيذاء الآخرين. والخبر الجيد هو أن ممارسة النظافة السايبرية الجيدة أسهل بكثير مما قد يبدو. وعلى الرغم من وجود الكثير من قوائم الممارسات المثالية المقترحة، فإنّ الحكومة الأسترالية قد لخصتها على نحوٍ مدهش في أربع استراتيجيات مفتاحية:

- القائمة البيضاء للتطبيقات: لا تسمح سوى للبرامج المجازة بشكلٍ صريح على نظامك وامنع جميع الملفات التنفيذية غير المعروفة وإجراءات التنصيب. سيتكفل ذلك بمنع البرمجيات الخبيثة والتطبيقات المؤذية من العمل.
- أصلح جميع برمجيات أجهزتك عبر تشغيل التحديثات البرمجيّة آلياً لبرامج مثل إم.إس أوفيس وجافا وقارئات بي.دي.إف وفلاش والمتصفحّات.
- أصلح ثغرات نظام التشغيل عبر تحديث نظامك، سواءٌ كان ويندوز أو ماك أو أندرويد، تلقائياً لتضمن أن ما تستخدمه هو نظامٌ تشغيل محّدث حتّى آخر إصدارٍ له طوال الوقت.

- قيّد الامتيازات الإدارية على حاسبك وحاول إمضاء معظم وقتك كمستخدمٍ عادي عندما تقرأ البريد الإلكتروني أو تتصفح الويب على سبيل المثال. ولا تسجّل الدخول كمدير إلى آلتك إلا حين تحتاج إلى ذلك، عندما تنصّب برمجيةً جيدة أو تجري تغييراتٍ على النظام على سبيل المثال. من شأن ذلك أن يحرم الأعداء امتيازات المدير، التي غالباً ما يحتاجون إليها لتنصيب البرمجيات الخبيثة والتفتيش في أنحاء شبكتك.

إن مجرد اتباع هذه الخطوات البسيطة كفيلٌ بتجنب نسبةٍ مدهشة من الاختراقات الموجهّة بلغت 85 بالمئة في دراسة الحكومة الأسترالية. كما كشفت دراسة معمّقة أجرتها فيريزون والاستخبارات الأميركية عن أخبارٍ جيدة مشابهة، حيث "أمكن تجنب 97 بالمئة من تسريبات البيانات عبر تطبيق قواعد بسيطة أو متوسطة". من شأن تحسين تصميم المنتج التقني وزيادة الوعي العام، أن يساهما في مساعدة الأفراد والشركات على حدٍّ سواء على اتخاذ الخيارات الصحيحة عندما يتعلق الأمر بالنظافة السايبرية. لكن للتعامل مع التهديدات الأخرى الأكثر إلحاحاً، لا بدّ من حلٍّ موحد شامل لها يستند إلى النماذج المعروفة في علم الأوبئة وانتشار الأمراض.

المركز السايبري للوقاية من الأمراض السارية: منظمة الصحّة العالمية في كوكبٍ شبكي

تعجّ اللغة التي نستخدمها في وصف حالة انعدام الأمن التقني لدينا بالمجازات التي تتصل بالمرض. فنحن نتحدث عن فيروسات الحاسب والإصابات التي يتعرض لها لوصف شيفرات برمجية خبيثة قادرة على التكاثر. لكننا في أغلب الأحيان، نلقي اللوم على أولئك الذين أصيبوا، بدلاً من التركيز على الوقاية والاكتشاف، لنحلّ الأمر رجعياً عبر اعتقال وملاحقة

أولئك المسؤولين بعد أن يكون الأذى قد وقع منذ وقت طويل. فماذا لو سحبنا هذا النظام قليلاً ونظرنا إلى مسألة الأمن السايبري العام الشامل على اعتبارها تمريناً في الصحة العامة؟ لقد قامت منظمات، مثل مراكز السيطرة على الأوبئة في أطلنطا ومنظمة الصحة العالمية في جنيف، على مدى عقود بتطوير أنظمةٍ متينة ومنهجيّات موضوعيّة للتعرّف على التهديدات التي تستهدف الصحة العامة والاستجابة لها، فتوصلت إلى بنى وأطر أكثر تطوراً بكثير مما يتوفر لدينا في الأوساط الأمنية السايبرية. نظراً لجميع هذه التقابلات بين الأمراض التي تنتقل بين البشر وتلك التي تصيب تقانات العالم، ثمة الكثير لنتعلمه من نموذج الصحة العامة، ذلك النظام المتكيف القادر على الاستجابة إلى طيفٍ لا ينفك يتغير من مسببات المرض في أنحاء العالم.

من الهام الإشارة إلى أن الإجراءات الفردية تبقى محدودة الأثر في مسائل الصحة العامة، فمن العظيم أن يكون لديك تقنياتٌ ممتازة للنظافة الشخصية، لكن إذا كانت قريتك مصابةً بأكملها بإيبولا، فإنك بدورك ستستسلم في النهاية. وهي مقارنةٌ واردة في عالمنا المحاط بالتهديدات السايبرية. فمن شأن المسؤولية الفردية والمبادرة أن تُحدِث فرقاً هائلاً في الأمن السايبري، لكن أملنا الوحيد في النهاية للاستجابة للتهديدات التي تنتشر كالنار في الهشيم عبر هذه المصفوفة الكوكبية من التقانات المتشابكة، هو في بناء معاهد جديدة تنسّق استجابتنا. فمن شأن "منظمة صحة عالمية" سايبرية دولية موثوقة أن تشجعّ التعاون والتنسيق بين الشركات والبلدان والوكالات الحكومية، وهي خطواتٌ حاسمة لا بد منها لتحسين الصحة العامة ككل في الشبكات التي توجّه البنى التحتية الحساسة في عالمينا المادي والافتراضي على حدٍّ سواء.

سيتكفّل مركز وقاية من الأمراض السارية بقطع شوطٍ كبير على طريق

مواجهة المخاطر التقانية التي تواجهنا اليوم، وقد يؤدي دوراً حاسماً في تحسين الصحة العامة ككل في شبكاتنا التي توجه البنى التحتيّة الحساسة في عالمنا. بل إن تقريراً نُشر برعاية مايكروسوفت ومعهد ايست ويست يقترح أنّ مثل هذا المركز السايبري قد يؤدي العديد من الأدوار التي تتم ممارستها اليوم ارتجالاً مثل:

- التوعية: أي تزويد الأفراد بطرائق مجربّة للنظافة السايبرية لحماية أنفسهم.
- مراقبة الشبكة: للكشف عن أية إصابات أو انتشارات للبرمجيات الخبيثة في الفضاء السايبري.
- الأوبئة: استخدام طرائق الصحة العامة لدراسة انتشار الأمراض الرقميّة وتقديم العون للاستجابة إليها والشفاء منها.
- المناعة: المساعدة على تلقيح العامة ضد التهديدات المعروفة عبر الإصلاحات البرمجية وتحديثات النظام.
- الاستجابة للحوادث: إرسال الخبراء عند الحاجة والتنسيق بين الجهود العالمية لعزل مصادر العدوى الشبكية ومعالجة المصابين.

على الرغم من وجود الكثير من المنظمات، الحكومية منها وغير الحكومية، التي تتولى المهام المذكورة أعلاه، فإنه ما من هيئةٍ تتولاها كلها بمفردها. وعبر هذه الفجوات في الجهود المبذولة وعمليات التنسيق بينها بالذات تستمر المخاطر السايبرية بالنمو. وما نحتاج إليه على وجه الخصوص هو التعامل المستوحى من علم الأوبئة مع المخاطر التقانية المتنامية للوصول إلى مصدر العدوى بالبرمجيات الخبيثة كما فعلنا في حربنا ضد الملاريا. فعلى مدى عقود كانت جميع الجهود الطبيّة تركز بلا جدوى على معالجة هذا المرض الطفيلي القاتل لدى أولئك المصابين سلفاً، ولم

يتحقق تقدمٌ حقيقي سوى عندما أدرك علماء الأوبئة أن المرض ينتشر بواسطة البعوض الذي يتكاثر في المستنقعات الراكدة في مكافحة المرض. وعبر تجفيف السبخات التي كانت تنمو فيها يرقات البعوض، حرمها علماء الأوبئة من أرضٍ خصبة هامة للتكاثر، ما خفّض انتشار الملاريا. فما هي المستنقعات التي يمكننا تجفيفها في الفضاء السايبري لتحقيق نتائج مشابهة؟ هذا هو ما لم نتوصل إليه بشكلٍ كامل حتى الآن وهو ما يمنح هذا العمل أهميته.

ثمة تحدٍّ كبير آخر سيواجهه مركز الأوبئة السايبري. فمعظم أولئك المرضى لا يعرفون أنهم يتجولون وهم مصابون، فهم ينشرون المرض بين الآخرين. فبينما يعاني مرضى الملاريا الحمى والتعّرق والغثيان وصعوبة في التنفس، هي كلها أعراض بارزة لمرضهم، ربما لا تظهر لدى مستخدمي الحاسب أية أعراض على الإطلاق. وتشهد على هذا الفرق الهام حقيقة أن الغالبية العظمى من الأجهزة المصابة لا تعلم مطلقاً بوجود برمجيةٍ خبيثة في آلاتها أو أنها مجنّدة في جيش شبكةٍ روبوتية. وحتى في عالم الشركات، مع زمنٍ وسطي لاكتشاف اختراقات الشبكة يصل اليوم إلى 210 أيام، فإن معظم الشركات ليست لديها فكرة عن أن أثمن أصولها، سواءٌ كانت الملكية الفكرية أم آلات المصنع، قد تم اختراقها.

الشيء الوحيد الأسوأ من أن يخترق المرء هو أن لا يكون على علم بذلك. فحين لا تكون على علمٍ بأنك مريض، كيف لك أن تتلقى العلاج؟ ثم كيف لنا أن نمنع انتشار الأمراض الرقميّة إذا كان حاملو هذه الأمراض لا يدركون أنهم يصيبون الآخرين بالعدوى؟ ستكون معالجة هذه القضايا ملفاً أساسياً لا بد من التعامل معه لأية منظمة صحة عالمية سايبرية يتم اقتراحها وهو الأساس لتحقيق السلامة المشتركة في المستقبل لنا ولِبُنانا التحتية المعلوماتية الحساسة.

كشف الباحث في مجال الأمن السايبري ميكو هوبنن عن عقب آخيل الواضح في عالمنا الحديث المشبع بالتقانة، إنها حقيقة أن كل شيء تديره الحواسب، وكل شيءٍ يعتمد على بقاء هذه الحواسب في حالة عمل. ويكمن التحدي الذي نواجهه في أنّ علينا ضمان طريقةٍ ما للاستمرار في العمل، حتى إذا انهارت الحواسب جميعها. فحين تنهار نظم معلوماتنا بالجملة، لن تكون هناك مداولاتٌ في أسواق المال ولن نتمكن من أخذ النقود من الصرافات الآليّة ولن تكون هناك شبكات هاتفية ولا محطات وقود. وإذا كُتب لهذه البنى الأساسيّة التي تشكل نواة مجتمعنا اليوم أن تختفي فجأةً، فماذا ستكون الخطة البديلة للبشريّة؟ إننا ببساطة لا نمتلك خطةً كهذه.

من شأن اتباع الخطوات المشروحة في هذا الفصل أن يقطع بنا شوطاً طويلاً في حماية أنفسنا من التهديدات التي تواجهنا اليوم، لكن خطة أفعالٍ كهذه أبعد من أن تكون مضمونةً. فنحن نشهد اليوم سباق تسلحٍ تقانياً، سباق تسلح بين من يستخدمون التقانة للخير ومن يستخدمونها للشر. ويكمن التحدي في كون الاستخدامات الخبيثة للتقانة تتوسع أسّياً بطرقٍ لا يمكن لأنظمة حمايتنا الحالية أن تواكبها ببساطة. لقد حان الوقت لتحقيق المزيد من المرونة في شبكة معلوماتنا العالمية تجنباً لتعرض النظام للانهيار. وإذا أردنا النجاة مع هذا التقدم الذي تفرضه تقاناتنا والتمتع بما تقدمه لنا من أفضالٍ سخيّة، لا بد لنا أولاً من تطوير تكيّفاتٍ أمنيّة قادرةٍ على مواكبة الوتيرة الأسّية للتهديدات التي نواجهها وتجاوزها. وما من وقتٍ نضيّعه.

الفصل الثامن عشر
الطريق القادمة

ليس على أحدٍ أن يقنُط معتقداً أن شخصاً واحداً لا يمكنه أن يفعل شيئاً إزاء المشكلات الهائلة التي تسود العالم من أمراض وبؤس وجهل وعنف. فقلةٌ هم من ستكتب لهم عظمة تغيير التاريخ، لكن بإمكان كلٍ منا أن يعمل على تغيير جزءٍ صغيرٍ من الأحداث. وسيشكل مجموع هذه الأفعال التاريخ المكتوب لجيلٍ كامل.

روبرت أف كينيدي

لا يمكن إعادة جُنّي التقانة إلى قُمقُمِه. فسواءٌ في الفضاء السايبري أم في الروبوتيات أم في الذكاء الصنعي أم في البيولوجيا التركيبية، ثمة تغييراتٌ هائلة تجتاح العالم. وقد أوصلتنا هذه التغييرات إلى امتطاء منحني أسّي سرعان ما سيصبح نموه انفجاراً خلال السنوات القادمة. بالفعل، فإنّ الفتوحات العلمية تصل على نحو أسرع بكثير مما كان معظمنا يعتقد. وكل مجالٍ من مجالات العلم يقود إلى تقدمٍ في مجالٍ آخر. فالتقدمات التي يتم تحقيقها في تقانة المعلومات تدفع البيولوجيا الحسابية بينما يدفع الذكاء الصنعي علم الروبوتيات. فكلٌ من هذه القوى تؤثر بالأخرى، ما ينتج عنه نموٌ أسّي للنمو الأسّي. وكما نوهنا خلال هذا الكتاب، لن تكون جميع هذه التطورات هادفةً إلى الخير. وقد وثقنا، مقدمين الأمثلة مثالاً تلو الآخر، كيف يقوم المجرمون والإرهابيون والقراصنة والحكومات المارقة بتخريب التقانة واستغلالها لإيذاء الآخرين. وليست الخلاصة بالطبع هي أنّ التقانة شريرة. فالنار، وهي التقانة الأصليّة، يمكن استخدامها لتدفئتنا ولطبخ طعامنا أو لحرق القرية المجاورة. وقد يحمل السكين جرّاح أو قاتل. وفي يد أولئك ذوي النوايا الحسنة ستأتي تقاناتنا السريعة التطور على العالم بازدهارٍ هائل. أما بين يدي انتحاري، فيبدو المستقبل مختلفاً تماماً.

أن تقيس هو أن تعرف.

لورد كيلفن

أحد أعظم التحديات التي نواجهها مع انعدام الآمن التقاني حالياً هو قلة أو انعدام المؤشرات على وجود دخلاء في شبكاتنا وأجهزتنا. فالمشكلة الواضحة هو أن لديك ضيوفاً غير مرغوب بهم (سواءٌ أدركت ذلك أم لا). واللغز الأعظم هو أنك لا تستطيع أن تحارب ما لا تراه. فمن هواتفنا الذكية إلى حواسبنا المحمولة واللوحيّة وحساباتنا المصرفيّة وثلاجاتنا وسياراتنا وشبكاتنا التجاريّة وشبكات الكهرباء، توجد أشباحٌ في آلاتنا. وإبقاء الدخلاء خارج شبكاتنا طوال الوقت هو هدفٌ سامٍ نصبو إليه. لكن ما فاتك هو أن الجمهوريّة التقانيّة التي نفخر بها قد سقطت. فتقانتنا تعجّ بالأخطاء والثغرات والغزاة. ومن المؤسف أنّ هدفنا اليوم لا يمكن أن يكون الوقاية المطلقة. فعلينا مطاردة الأشباح وطردها من آلاتنا عبر البحث عنها على نحوٍ فعال وإسقاطها. ومع الوقت الوسطي لاكتشاف الهجوم الذي يبلغ أكثر من مئتي يوم، من الواضح أنه ثمة الكثير لنقوم به. فعلينا خفض هذا النطاق الزمني بحيث يكون بضع ساعاتٍ فقط، بل ليصل في النهاية إلى دقائق أو ثوانٍ.

تبقى المشكلة المستمرة مع البيانات الكبيرة، هو أنه كلما احتفظت بقدرٍ أكبر من البيانات زادت مسؤوليتك في الحماية. لكن معظم الشركات لم تقم ولو مرةً واحدة بتصنيف أصولها المعلوماتية بحيث تتمكن من تحديد طبيعة البيانات التي تخزنها ومعرفة أماكن تخزينها وانتقاء البيانات الأكثر حساّسية التي لا بد من حمايتها. وحين يتم اكتشاف هذه التهديدات، فمن

الهام جداً أن نبدأ بمناقشتها علناً.

إن تحطيم جدار الصمت الذي يحيط بمعظم الهجمات السايبرية هو خطوةٌ حاسمة لدعم أمننا التقاني المشترك. فالشركات تعلم اليوم عواقب تسميتها علناً كضحية اختراق. فبعيداً من تضرّر السمعة الواضح، قد تصل التكاليف إلى مئات الملايين من الدولارات على شكل خسائر مباشرة وضياع للزبائن ودعاوى قضائيّة. لذا فإن المنظمات ستفعل كل ما بوسعها للحفاظ على الصمت حين تقع ضحيةً، سواءٌ لشركة الجريمة أو لوكالات التجسس الأجنبية. لكن هذا الصمت يشكل مشكلةً جوهريّة لأمننا السايبري. فحين ينجو شخصٌ من اعتداءٍ جنسي، لكنه يشعر بالإحراج والخجل إلى حدّ أنّه لا يبلغ الشرطة به، فإنّ المعتدي لن يُكتشف ولن يُلاحق، وسيبقى حرًّا ليوقع بالتأكيد مزيداً من الضحايا. ومع أن الهجوم السايبري هو شكلٌ مختلفٌ تماماً من الجريمة، فإن ضحاياه أيضاً يكرهون التحدّث علناً. لذا فإنّه من غير الممكن تجميع هذه الحوادث ودراستها، كما يتعّذر بناء دفاعاتٍ مشتركة ويبقى المهاجمون يتسكّعون بحريّة في انتظار هجومهم القادم غداً. لا بدّ لنا من تصحيح هذا الوضع. فالتزام الصمت حيال هذه المخاطر لا يجعلها تختفي، بل يزيد الطين بلّةً، ويمنح الحصانة للأطراف السيئة. فتماماً كما تقرّر اللجوء إلى خط مساعدة الكحوليين مُغفل الهوية، يمثل الاعتراف بأن لديك مشكلةً سايبرية أول وأهم خطوة على طريق المعالجة.

تحقيق المرونة: أتمتة الدفاعات والتوسّع من أجل الخير

> يمكن استخدام التقانات الجديدة لأهدافٍ تدميرية. والحل هو في تطوير نظم سريعة الرد لمواجهة الأخطار الجديدة كقيام إرهابي بيولوجي بخلق فيروس بيولوجي جديد.
>
> راي كورزوايل

الهجمات السايبرية تحدث، ولا يمكن إيقافها كلها. لذا فإن السؤال الأهم

الواجب طرحه هو كيف يمكننا بناء عالمنا التقاني الذي يتطور بسرعةٍ بطريقةٍ يُصبح معها سريع الاستجابة لمثل هذا الهجوم؟ إنه سؤال ليس من السهل الإجابة عنه نظراً لتعقيدات النظام الذي لا ينفك يتوسّع. فالنظام المرن هو نظامٌ لن ينهار على نحوٍ كارثي، بل سيخبو ببطءٍ مع الوقت إلى أن يصبح بالإمكان إصلاحه. وسيستمر النظام المرن بتنفيذ معظم وظائفة الحساسّة، وإن خرجت نشاطاتٌ أقلّ أهمية عن الشبكة أو توقفت عن العمل. ولدى الطبيعة بنيةٌ ممتازة تحقّق هذه الشروط تشهدُ عليها السحليّة العاديّة. فحين تتعرض السحليّة للهجوم، أو يمسك بها حيوانٌ مفترس، يمكن لها بسهولة أن تتخلّص من ذيلها الذي سينمو مجدداً، ما يسمح لأعضاء الجسد الهامة (كالدماغ والأعضاء التناسلية) بالهرب والنجاة. فما هو ذيل السحليّة في الإنترنت أو في شبكة شركتك؟ إنه غير موجودٍ بعد، وهو شيءٌ لا بدّ لنا من تغييره.

تعاني معظم بنانا التحتيّة التقانيّة نقاط القصور المفردة الشائعة، وربما كانت أوضحها هي الطاقة. فمن دون طاقة لا إنترنت. والأسوأ هو أنه من دون كهرباء سيتوقف توزيع الماء وإنتاج الطعام والمناقلات المالية والاتصالات والنقل. فعلينا عزل نقاط القصور هذه بحيث لا تنتشر، كما أن علينا إيجاد مصادر طاقة بديلة قابلة للتوسع لمنع هذا النوع من "انقطاع الكهرباء"، ليس فقط للكهرباء بالطبع، بل لجميع الأدوات التقانية التي تجعل حضارتنا الحديثة ممكنة.

لا تقف هذه المخاطر عند شبكة الطاقة، بل تتجاوزها لتشمل معظم أنظمة البرمجيات الشائعة لدينا، بل البنية التحتية للإنترنت أيضاً. فالكثير من الأدوات التي تشّغل عالمنا التقني أحادية الزراعة بطبيعتها، أي إنها تعتمد على برمجياتٍ متطابقة تقريباً وتحتوي الثغرات نفسها. فالزراعة الأحاديّة الحاسوبية، على غرار تلك المعروفة في مجال الزراعة، عُرضةٌ

لانهيار كارثي، كما حدث في مجاعة البطاطا الإيرلنديّة. فنظام ويندوز من مايكروسوفت يشّغل اليوم أكثر من 90 بالمئة من الحواسب المكتبيّة في العالم، وحتى بداية عام 2014 كانت نسبة مدهشة من الصرافات الآلية في الولايات المتحدة بلغت 95 بالمئة لا تزال تعمل على نظام ويندوز إكس.بي، وهو نظام التشغيل الذي أوقفت مايركوسوفت جميع تحديثاته الأمنيّة. إن الزراعة الأحاديّة التقانيّة هي الدماء التي تمنح الحياة لهجمات الحاسب الجماهيرية. فباستخدام برمجيةٍ خبيثة واحدة يمكن للقراصنة إحداث أثر عالمي عميق، عبر جعل جميع نسخ برمجيةٍ معينة تنهار بالطريقة ذاتها. وكما رأينا، فإنّ الثغرات المعروفة تبقى حيّةً في أنظمتها لسنواتٍ قبل أن يقوم بائعو البرمجيات بسدّها. وحالما يُكتشف اختراقٌ لنسخةٍ ما من ويندوز 8 أو قارئ البي.دي.إف من آدوب، يجب أن تبدأ عملية إصلاح عالمية. وعلى شركات البرمجيات أن لا تنتظر الناس حتى يقوموا بإصلاح أنظمتهم يدوياً (ونحن نعلم أن معظمهم لا يفعل). بل على هذه الأنظمة أن تكون قادرةً على شفاء نفسها بحيث تبحث دائماً عن آخر الإصدارات المحسّنة من البرمجيات، لتضمن بقاء جميع الأبواب والنوافذ التي تقود إلى حياتنا الرقميّة موصدة. بعبارةٍ أخرى فإن الفشل في معالجة نقاط ضعفٍ معروفة في عشرات الملايين من النسخ من البرمجية نفسها التي تعمل في أنحاء العالم، أشبه باكتشاف الخطأ الميكانيكي الذي أدى إلى تحطم طائرة البوينغ747، ذلك الخطأ الموجود في جميع الطائرات العاملة عالمياً من هذا الطراز، وترك هذه الطائرات تستمرّ في الطيران.

علينا أيضاً أن نضمن إمكانية عزل الاختراقات والهجمات المفردة ومنعها من الانتشار. ولنأخذ هجوم عام 2013 على عملاق تجارة التجزئة تارغت مثالاً. فكما ذكرنا سابقاً، تمكن المهاجمون المسؤولون عن ذلك الهجوم من الوصول إلى طرفيات نقاط البيع لدى تارغت، عبر اختراق شبكة المتعاقد

المسؤول عن إصلاح نظم التدفئة والتكييف في المتجر أولاً. ولو أمكن اكتشاف هذا الاختراق لأمكن تجنّب الكابوس الأمني التجاري الذي حلّ بمتاجر تارغت كلياً. إننا بحاجةٍ إلى طرقٍ أفضل وأكثر مرونة لحماية معلوماتنا تكون أشبه بأكياس الهواء الخاصّة بالبيانات. فحين يحدث اختراقٌ للبيانات، على أكياس الهواء الافتراضيّة هذه أن تنطلق وتُغلِف ممتلكاتنا الرقمية لحمايتها من أي أذىً قد يحدث بعد ذلك.

على المديرين التنفيذيين وهيئات الإدارة أن يسألوا أنفسهم عن مدى مرونة منظماتهم. فالمرونة تعني البقاء في حالة عمل حتى في حال وقوع هجومٍ قوي يشنّه أعداءٌ متقدمون. فمع أنك، كما السحلية، قد تفقد ذنبك، على المنظمة أن تستمر في الحياة. وهو أمرٌ لن يحدث بسحر ساحر ويتطلب تدريباتٍ وتمارين على الجاهزية. وتحتاج المرونة السايبرية على وجه الخصوص إلى مهارةٍ في الاستجابة للهجوم والخفّة في استعادة القدرات التقانية المصابة بسرعة. وربما تكون القدرة على الشفاء بسرعة بعد الهجوم مسألة حياةٍ أو موت تقرّر ما إذا كانت المنظمة ستنهار أم ستنجو. أما الوقت المناسب للإجابة على هذه الأسئلة فهو ليس خلال الأزمة بل قبل حدوثها بوقتٍ طويل. ولا بدّ من بناء هذه الأنظمة الأكثر مرونة التي نطالب بها ابتداءً بالأسس. إذ لا يمكن للأمن أن يكون فكرةً لاحقة ترمى في الخليط بعد أن تكون الآلات قد بنيت وانتهى الأمر. بل تجب هندسة الأنظمة بحيث تنهار بلطف لا على نحوٍ كارثي. وعلى الحوسبة الآمنة الموثوقة أن تكون حجر الزاوية في مستقبلنا التقاني إذا ما أردنا لنظامنا أن لا ينهار برمّته. وهو ما يصحّ أكثر بعد مع انتقالنا نحو إنترنت الأشياء، ومع وصول تقاناتٍ ستحدث تغييراً كبيراً كالروبوتيات والذكاء الصنعي وتقانة النانو. لم يعد بإمكاننا تجاهل الآثار السياسيّة والقانونيّة والأخلاقيّة والاجتماعيّة للأدوات التقانيّة السريعة النمو التي نقوم بتطويرها. فنحن

مسؤولون أخلاقياً عن اختراعاتنا.

ثمة أمثلةٌ تاريخية جيدة وقفنا فيها كمجتمعٍ وجمعنا تجاربنا توقعاً لخطرٍ كارثي قبل حدوثه. ومن ذلك ما حدث عام 1975 في مؤتمر أزيلومار حول الـ دي.إن.إيي التركيبي، الذي عقد على شاطئ أزيلومار في مونتري بكاليفورنيا. فقد جمع المؤتمر بين 140 عالم بيولوجياً وطبيباً ومحامياً وعالماً بالأخلاق لمناقشة الأخطار البيولوجية التي قد تصحب تقانات الـ دي.إن.إيي الناشئة، ولوضع خطوط سلامة طوعيّة. وتمخّض عن الحدث اتفاق العلماء على وقف التجارب التي تشتمل على مزج الأحماض الريبية النووية العائدة لمتعضيّات مختلفة. وهو مجال بحثٍ اعتبر في ذلك الوقت محمّلاً بعواقب متطرفة غير مدركة وقد تكون كارثية. وكانت دروس ونجاحات أزيلومار شيئاً يستحق تكراره. فمع أننا نسابق بما أوتينا من قوة للتقدم بالبيولوجيا التركيبية والذكاء الصنعي والروبوتيات السربية وتقانة النانو، فإننا نخصص القليل من الموارد الثمينة لفهم المخاطر التي ترافق التقانات والتي قد تتضاعف بحيث تخرج عن سيطرتنا. ولحسن الحظ فإنّ اجتماعاً حول مستقبل الذكاء الصنعي قد عُقد على الشاطئ نفسه في مونتري، ومثل هذه الاجتماعات تمثل الأساس في دعم القدرة على الرد في عالمٍ مبني على التقانات الأسّية.

لننظر إلى الأمام، فإننا إذا أردنا تقوية السلامة والأمن في مجتمعنا لا بدّ لنا من القيام بتغييرٍ آخر. فلعينا أن نكون قادرين على الاستجابة على قدر التحدي الذي نواجهه والذي يفرضه علينا وسطٌ مؤتمت بشكل كامل من القراصنة المجرمين. وقد سبق لنا أن رأينا ذوي النوايا السيئة يؤتمتون هجماتهم المرّة تلو الأخرى. وهذه القدرة بالذات هي التي أحدثت قفزةً في مدرسة الجريمة انتقلت بها من العمليات الفردية إلى العمليات الشاملة. وهو ما يسمح لعصابة إجراميّة منظمّة واحدة بجمع 1.2 مليار كلمة مرور،

بينما تقوم عصابةٌ أخرى بشنّ حملة حجب خدمة تضّخ خلالها 70 غيغابايت في الثانية تدكّ بها أكثر من عشر مؤسساتٍ مالية وتخرجها من الشبكة. فأدوات ارتكاب الشر تتوسّع أسّياً، بينما أنظمتنا التي تهدف إلى الخير لا تستطيع المواكبة. فدفاعاتنا لا تتكيف بسرعةٍ تكفي لمواكبة الخطر المنظّم العالمي الذي نواجهه، وهو أمرٌ حريّ بحكومتنا أن تشعر ببالغ القلق إزاءه.

إعادة اختراع الحكومة: ابتكار الانطلاقة السريعة

لا يمكننا حل المشكلات بطريقة التفكير نفسها التي استخدمناها حين خلقنا هذه المشكلات.
ألبرت أينشتاين

عام 2014 كان 13 بالمئة من الأميركيين فقط راضين عن عمل الكونغرس، في تحسّنٍ طفيف مقارنةً بنسبة التسعة بالمئة المنخفضة التي بقيت مسيطرةً في تشرين الثاني عام 2013. فالثقة بالحكومة غير موجودة عملياً، سواءٌ كان الأمر يتعلق بالأموال في السياسة أو تعطلات الحكومة أو التحّيز أو نُدرة التشريعات المفيدة. وبينما يستمر التغير التقاني من حولنا بوتيرةٍ أسّية، تبقى الحكومة مصرّةً على وتيرتها الخطيّة في التغير. والتحدي الواضح الذي يفرضه هذا الخلل هو أننا لن نتمكن من حل مشكلات القرن الحادي والعشرين بمؤسسات القرن التاسع عشر. فنحن بحاجةٍ إلى حكومةٍ أكثر قدرةً بكثير على التكيّف، حكومةٍ تستجيب أسرع بعشر مرات، وذلك فقط لتضمن استمراريتها. فأمناء سرّ الوزارة وقضاة المحكمة العليا الذين "لا يستخدمون البريد الإلكتروني ببساطة" لم يعد لهم نفع.

لا يقتصر نقص الإبداع في الحكومة على المشرّعين فقط، بل إنه ينخر في أجهزة الأمن الوطني والسلطة التنفيذية. فاستجابةً للإبداع (وإن كان شيطانياً) الذي أظهره منفذو هجمات الحادي عشر من أيلول، أنفقت

الحكومة مليارات الدولارات وخرجت علينا بـ "إبداعاتٍ" مثل إدارة أمن النقل. ومع أنه لا بأس من تفتيش أطفالٍ في الرابعة أو عجائز على كرسيٍّ متحرك إذا ما أراد المرء أن يخرج "مسرحيةً أمنيّة"، فإنّ علينا أن نحسّن شروط لعبتنا تحسيناً كبيراً إذا كان لدينا أملٌ في منع الهجمات الإرهابيّة في المستقبل. فنظراً لوتيرة التقدم التقاني، لن تكون التهديدات الأمنيّة في الغد مثل تلك التي نشهدها اليوم، وهو أحد الأسباب التي تجعل الحكومة تصارع بما أوتيت من قوة للتخلص من انعدام الأمن السايبري الشائع لدينا.

ليس المقصود بذلك بالطبع أنه ما من إبداعٍ لدى الحكومة. فالحكومة هي التي أحضرت إلينا الإنترنت والسفر في الفضاء وكانت هي من حفّز ترميز الجين البشري أخيراً. فثمة جيوبٌ للإبداع لدى الحكومة في كل مكان، لكننا نحتاج إلى جعل هذه الدُرر الإبداعيّة تتضاعف وتتوسع بطريقةٍ لسنا نراها اليوم بكل بساطة. ومن هذه النماذج منظمة "شيفرة أميركا"، وهي منظمةٌ غير ربحية تنظّم المتطوعين من المواطنين ذوي المهارات في برمجة الحاسب لجعل الخدمات الحكومية أكثر بساطةً وفعاليةً وأسهل استخداماً. والنموذج الآخر هو مختبر غوفلاب الإبداعي في جامعة نيويورك، الذي يكرّس نفسه لاستخدام التقانة لإعادة تصميم عملية حل المشكلات في المؤسسات الحكومية. ويعمل المختبر، المدعوم من قبل ماك.آرثر ومؤسسات نايت، على استخدام التقانات الشبكية لتجاوز نماذج التحكم المركزية الموجّهة من القمة إلى القاعدة التي كانت سائدةً بالأمس لصالح منصّات أكثر تحولاً تعتمد على الحكم الذاتي والإبداع وانخراط المواطنين.

في الواقع، فإن الحكومة إذا أرادت أن تحتفظ بدورٍ لها في التحديات الأكثر ضغطاً وإلحاحاً التي يواجهها العالم اليوم، فعليها أن تتوصل إلى أطر جديدة كلياً لحل المشكلات. ويمكننا في هذا الصدد استعارة صفحةٍ من وادي السيليكون بأن نبدأ بالتفكير في نظام الحكم لدنيا على أنه نظام

التشغيل الخاص بالمجتمع. فإذا كان بمقدورنا تغيير أسس نظام التشغيل، فسيتغير كل شيءٍ معه. فمؤسساتنا الموروثة لديها معاناة، سواءٌ في مجال التعليم أو الرعاية الصحيّة أو تطبيق القانون، والتقانة تتجاوز الحكومة وقدرتها على الاستجابة. فحتى اليوم تبقى منهجية الحكومة في التعامل مع الأمن التقاني في جُلّها مجرد واجهة مزيّنة وفرصٍ ضائعة. ونحن بحاجةٍ إلى نظام تشغيلٍ جديدٍ للعالم، نظامٍ مبني على المبادئ الأولى وقادرٍ على مواكبة التغيرات الأسّية الجارية من حولنا.

ثمة مقولة مشهورة لبيل جوي هي "أيًّا كُنت، فإنّ معظم الأذكياء يعملون لدى شخصٍ آخر". وعلى الرغم من أن تعليقه هذا كان مُوجّهاً في الأصل إلى العالم التجاري، فإنه مقولته تنطبق على الحكومة بالقدر نفسه، وربما أكثر. فمن الواضح أن المؤسسات الحكومية اليوم لا تحتكر حلول الكثير من المشكلات التي نواجهها اليوم، لكنها تستطيع تأدية دورٍ هام كداعية يجمع بين القطاعين العام والخاص كوسيلةٍ لإيجاد الحلول لبعض أعظم التحديات التي تواجهنا.

الشراكة العامة - الخاصة الجادة

لطالما كانت محاولات الحكومة لحماية الناس ضد الجريمة السايبرية اليومية والتهديدات الأمنيّة غير مناسبةٍ على الإطلاق. وهل يفاجئنا ذلك؟ إن عشرات الآلاف من الهجمات الناجحة التي تستهدف واشنطن ويشنّها أعداء أجانب، تثبت أن الحكومة الأميركية لا يمكنها حتى أن تحمي نفسها. فالحاجة واضحةٌ إلى تعاون أكثر جديّة وعمقاً بين القطاعين العام والخاص. فمن دونه، لن يكتب لنا كبيرُ تقدمٍ في تحسين الحالة الأمنيّة العامة لدينا. وتصبح هذه الحاجة أكثر إلحاحاً حين يتعلق الأمر بالبنى التحتيّة الحساسة للبلاد، والتي يقع 85 بالمئة منها بين يدي القطاع الخاص. فنحن كأمّةٍ وكشعبٍ بحاجةٍ إلى تعاون الحكومة والصناعة لحماية آلات عالمنا الحديث.

ويبقى السؤال هو كيف.

إدراكاً منها للحاجة إلى شراكاتٍ بين القطاعين العام والخاص، قامت مؤسساتٌ متنوعة، منها مكتب التحقيقات الفيدرالي والاتحاد الأوروبي والمنتدى الاقتصادي العالمي، بتكريس برامج تشّجع على مزيدٍ من التعاون بين أولئك المسؤولين عن تطوير البنى التحتية الحساسة للعالم. وثمة مبادراتٌ أخرى، مثل مراكز مشاركة المعلومات وتحليلها، تمكّن صناعاتٍ معينّة، مثل الخدمات المالية أو الطاقة أو الاتصالات، من تحسين تعاونها وقدرتها على الاستجابة للتهديدات السايبرية. كما يؤدي "منتدى الاستجابة للحوادث والفرق الأمنيّة" دوراً بارزاً في تحسين التنسيق والاستجابة بين الأطراف الموثوقة في كلٍ من الحكومة والقطاع الخاص، عبر فرق الاستجابة الطارئة الحاسوبية. لقد أثبتت الجهود الأوليّة المبذولة لتحقيق الشراكات الأمنيّة العامة - الخاصّة فائدتها بلا شك، لكن بعضها انتُقد لغموض تعريف أهدافه وقلةٌ منها، إن وجدت، تمكنت من تحديد أهدافٍ واضحة لها تتجاوز "مشاركة المعلومات".

ثمة مشكلاتٍ حقيقية لا بد من التغلب عليها لجعل تشارك المعلومات العامة - الخاصة يحقق أقصى فائدةٍ ممكنة. فالقطاع الخاص عموماً لا يثق بقدرة الحكومة في الحفاظ على سرّيته، تحديداً حين يتعلق الأمر بالكشف عن بيانات التهديدات السايبرية لمنافسيه، ناهيك بحمايتها من خطر مكافحة الاحتكار. وللحكومة أيضاً تحدياتها، فعليها أن تجد طريقة لمشاركة المعلومات حول مخاطر سايبرية معينة، تكون معظمها سريةً مع غياب التصريحات التي تسمح للشركات والكوادر التقنية بالوصول إلى الموادّ السرّية. ففي تقريرٍ لمكتب المسؤولية الحكومية عام 2010 تبيّن أن أقل من ثلث الشركات المشاركة في برامج التعاون الأمني السايبري مع الحكومة، كانت تتلقى معلوماتٍ عن التهديدات السايبرية تستوجب إقامة دعاوي

قضائية.

إذا ما أردنا التغلب على المخاطر التقانية الهائلة القادمة إلينا، فلا بدّ لنا من التغلب على هذه الآفات بمزيدٍ من الجديّة، بما يشجّع على بناء شراكاتٍ مثمرة بين الحكومة والقطاع الخاص.

من التجارب الإيجابية على نحوٍ لافت في هذا المضمار شبكة سي نت (شبكة الإبداع الأمني) التي تهدف إلى تشجيع الإبداع في مجال الأمن السايبري، عبر بناء جسورٍ جادّة بين القطاعين الحكومي والخاص. وقد تمّ تأسيس سي نت في سان فرانسيسكو لتؤدي دور الوصلة (أو كالمترجم) بين أولئك في وادي السيليكون والآخرين في النطاق الحكومي. فمن خلال جمعها بين هؤلاء اللاعبين الكبار من كلا العالمين، ساعدت سي نت على دعم المبادرة والإبداع بين جميع الأطراف العاملة ضمن البيئة الأمنية السايبرية بحيث تركز على المهمة التي تعمل عليها. وبعيداً من أولئك العاملين في الحكومة والصناعة الذين يجعلون من محاربة التهديدات السايبرية شغلهم الشاغل بدوامٍ كامل، ثمة قوةٌ جماهيرية يمكن تفعليها لتحمّل بعض العبء في مواجهتنا للتحديات التقانية، إنّه الجمهور الواعي والملتزم من العامّة.

نحن الشعب

ليس إيماننا بالتقانة بل بالناس.

ستيف جوبز

من شأن التأمل في حجم ومدى النشاطات الخبيثة التي تُرتكب من قبل المجرمين المنظمين والإرهابيين والقراصنة والحكومات المارقة، أن يدفع المرء إلى الإحباط والخوف، بل حتى إلى الاكتئاب. لكن إذا كان هنالك شيءٌ واحد يعزّيني بعد عقدين من العمل في مجال الأمن العام، فهو في أن الأخيار يفوقون في أعدادهم الأشرار في العالم. إنها نقطة قوةٍ هائلة، لكن أحداً منا

لم يستغلها لمصلحتنا بشكلٍ كامل بعد. تمتاز شركة الجريمة بمهارةٍ كبيرة في التعهيد الجماهيري، وهي قادرةٌ على تعبئة غوغاءٍ بالآلاف، كما رأينا الهجوم السايبري الذي استهدف الصرافات الآلية عام 2013، في حملةٍ شاملة نفذها لصوصٌ قاموا شخصياً بتنفيذ 36 ألف مناقلة في غضون عشر ساعات، عبر 27 بلداً أدخلت إلى جيوبهم مبلغاً لا بأس به وصل إلى 45 مليون دولار. إنه هجومٍ مدهش في سرعته ومهارته وابتكاره وأثره. فما الذي يكافئ هذا المستوى في مجال السلامة العامة؟ لا شيء، وهذا شيءٌ لا بدّ لنا من تغييره إذا ما أردنا تدعيم دفاعاتنا الذاتية وقدرتنا على الاستجابة في فجر العصر الرقمي هذا.

بات واضحاً لي إلى حد مؤلم، أنّ السلطات تخسر تفوقها التقاني لمصلحة المجرمين. فالسلطة التنفيذية الغارقة في أعباء عملها والرازحة تحت خفوضات الميزانية، تتعرض للهجوم وتصارع من أجل المواكبة بما أوتيت من قوة. علاوةً على ذلك، تمثل الشرطة نظاماً مغلقاً، فهي تبقى في نطاق البلد، فيما تأتي التهديدات عابرةً للدول. لقد أصبحت نماذجنا الحالية للتعاطي مع الأمن من خلال الأسلحة وحرس الحدود والأسوار العالية، باليةً إلى حدٍّ صادم. فهي غير قادرة على منع دخول البتّات والبايتات التي تتنقل في أنحاء العالم بسرعة الضوء. وللتغلب على هذه العقبات الواضحة التي تعانيها مؤسسات السلامة العامة الحالية، لا بدّ لنا من إيجاد طرق جديدة ثورية لمعالجة المشكلة، طرقٍ تشتمل على أشكال أكثر انفتاحاً وتعميماً للمشاركة في محاربة الجريمة. فأين هي برامج مراقبة الحي والدوريات المحلية في الفضاء السايبري؟ بدلاً من بناء قوةٍ نخبوية صغيرة من العملاء ذوي التدريب العالي لحمايتنا جميعاً، سيكون من الأفضل لنا تمكين المواطنين العاديين من التغلب على المشكلة كمجموعة عبر التعهيد الجماهيري. فللتغلب على شركة الجريمة في لعبتها يجب أن نتمكن من

التوسع مع المحافظة على الجودة.

ليست فكرة التعهيد الجماهيري لتطبيق القانون جديدةً تماماً. ففي عام 1، عندما اغتال جون ويلكس بوث الرئيس لينكولن، أصبح أول مجرم هاربٍ تنشر صوره على إعلانات المطلوبين. أما اليوم، وبعد 150 سنة على اغتيال الرئيس السادس عشر للبلاد، بالكاد تغير أسلوب الحكومة في التعهيد الجماهيري لتطبيق القانون. حيث يقوم رجال الشرطة بتوزيع الصور على قنوات الأخبار المحليّة لتقوم المحطات بتحذير الناس من أنّ الشخص المطلوب "مسلح وخطير. يرجى الاتصال بالسلطات المحليّة إذا شاهدتموه". حقًّا؟ في عام 2015 يمكننا بلا شك أن نقوم بشيءٍ أفضل لحفز التعاون الشعبي أكثر من "إذا رأيت شيئاً قل شيئاً".

نحن الشعب، تماماً كما شركة الجريمة، يمكننا الاستفادة من التوفر السخي للتقانة بما يساعدنا على حماية أنفسنا والدفاع عنها. يستخدم كلي شيركي مصطلح "الفائض الإدراكي" لوصف قدرة سكان العالم على التطوع والمساهمة والتعاون في مشاريع كبيرة، بل عالمية. إنها اللحظة المناسبة لنبدأ نحن الشعب باستخدام الفائض الإدراكي المتوفر لدينا لنساعد في حماية مستقبلنا والدفاع عنه. ولا بدّ من مواجهة الأسلحة المفتوحة المصدر والجريمة المعتمدة على التعهيد الجماهيري، بأدوات الأمن المفتوحة المصدر والسلامة العامة المعتمدة على التعهيد الجماهيري. ولحسن الحظ، ثمة بعض النقاط المضيئة التي تبشّر ببداية هذا العهد الجديد من السلامة العامة. فثمة منظماتٌ مثل كرايزس كومونز وأوشاهيدي، تعمل على إعادة اختراع عمليات الإغاثة في حالات الكوارث وإنقاذ الأرواح، عبر تنسيق ردود فعل المواطنين على حالات الطوارئ العامة، كزلزال هاييتي والهجوم الإرهابي على مركز ويست غيت للتسوق في نيروبي. إذ يستخدم المواطنون في المكسيك، البلد الذي اجتاحته 50 ألف عملية اغتيال متعلقة بعصابات

المخدرات بين عام 2006 و2012، باستخدام خرائط غوغل للإبلاغ عن طريق التعهيد الجماهيري عن العصابات ونشاطاتها ومواقعها. وفي أوروبا الشرقية، يجمع مشروع الإبلاغ عن الجريمة المنظمة والفساد بين الصحافيين والمواطنين ويطبق التعهيد الجماهيري لإجراء تحقيقاتٍ معقدة عابرة للأمم، للكشف عن الديكتاتوريات والمسؤولين الفاسدين والإرهابيين وعصابات الجريمة المنظمة التي تحرّك أو تغسل أرباحها الكبيرة التي حصلت عليها بطريقةٍ غير مشروعة عبر الكوكب. وعلى ذكر الفساد العام، قام محررون في جريدة الغارديان عام 2009 في بريطانيا بتطوير برمجيةٍ تسمح للمواطنين بـ "التحقيق الجماهيري" في أكثر من 455 ألف صفحة من البيانات، كانوا قد حصلوا عليها بهدف اكتشاف أي انتهاكاتٍ كبيرة لطلبات استرداد النفقات من قبل أعضاء البرلمان البريطاني. وانضم أكثر من 25 ألف متطوع من المواطنين إلى هذه التحقيقات الرقميّة، وكانت النتائج مذهلةً بحق. فقد تمّت مراجعة أكثر من 170 ألف وثيقة في الساعات الثمانين الأولى. وأدى اكتشاف الجمهور لآلاف الاختلاسات الكبيرة من المال العام، إلى إجبار العديد من أعضاء البرلمان إلى الاستقالة إضافةً إلى بعض الوزراء، بل حتى الناطق باسم مجلس العموم، إنها نتيجةٌ مذهلة حقاً لم نرها منذ عام 1695.

في كلٍ من هذه الحالات، كان بإمكان الأفراد أن يقدموا ما هو أكثر من مجرد إبلاغ السلطات بالجرائم. فقد تمكنوا من تقديم الأدلة عبر حشد الوقت والطاقة لفك تشفير البيانات والخروج بنتائج بسرعةٍ لا يمكن أن يحققها أي جهاز شرطةٍ أو منظمةٍ حكومية بمفردها. فمن شأن التعهيد الجماهيري للسلامة العامة أن يوصلنا إلى نتائج واضحة، ولا بد من جعله جزءاً أساسياً من استراتيجتنا للأمن العالمي، في عالمٍ يتغير تغيراً أسّياً ويتميز بالعوز إلى كوادر الأمن السايبري المتفرغة. وقد نوهت مؤسسة راند، إلى أن

النقص في محترفي الأمن التقني على مستوى البلاد ضمن الحكومة الفيدرالية، بات حرجاً إلى درجة أنه يعرض أمننا الوطني والداخلي على حدٍّ سواء للخطر. وتردد صدى هذه النتائج في تقرير الأمن السنوي الذي أصدرته سيسكو عام 2014، والذي قدّر النقص في الكوادر بأكثر من مليون محترف أمن سايبري على مستوى العالمي، متوقعةً نمو هذا العدد إلى مليونين بحلول عام 2017. إننا بحاجةٍ ماسّة إلى مزيدٍ من التعاون الشعبي لحماية مستقبلنا التقاني، وهو ما بدأت حتى القنوات الرسمية الاعتراف به.

اعتبر كبير المحامين السايبريين لمكتب التحقيقات الفيدرالي، ستيفن شابنسكي، عام 2012 جهود الحكومة في مجال مكافحة الجريمة السايبرية، "طريقةً فاشلة"، وأضاف أنه لا بد من بذل جهودٍ أكبر بكثير من قبل أفراد الشعب لمكافحة التهديدات السايبرية. وهو عملٌ بدأ ينطلق ببطء. فقد حدث ذات مرة أن عمل أستاذٌ في جامعة ألاباما مع طلابه في مقرر العدالة الجنائية لمساعدة مكتب التحقيقات الفيدرالي، في الإيقاع بعصابة جريمةٍ سايبرية تمتلك 70 مليون دولار وتديرها شركةٌ إجراميّة انطلاقاً من أوكرانيا وروسيا. وقد نجحت "التحقيقات الجماهيرية" التي أجراها الطلاب في التعرّف على العديد من المشتبه بهم في الولايات المتحدة، الذين كانوا يستخدمون حصان طروادة المصرفي زيوس لسرقة الملايين، وقد تمّ في النهاية إلقاء القبض على هؤلاء الأفراد من قبل مكتب التحقيقات الفيدرالي بفضل لعمل الطلاب. لكن إذا أردنا أن نحقق نجاحاً ذا أثر على المدى البعيد، فلا بد من أن تصبح جهود التعهيد الجماهيري جزءاً من صيغة النظام لكي نتمكن من توسيعها بدلاً من بقائها مجرّد إجراءٍ مؤقت. وقد قامت الشرطة في المملكة المتحدة عام 2011 بخطوةٍ في هذا الاتجاه عبر إنشاء كادرٍ وطني من رجال الشرطة المتطوعين، الذين يمتازون بالمؤهلات المطلوبة للمساعدة في مكافحة الجريمة السايبرية.

علينا نحن، هنا في الولايات المتحدة وفي الأماكن الأخرى من العالم، أن نبني على هذه النجاحات وأن نمضي بها قدماً. فلدينا رجال شرطة احتياطيون ومساعدون. وفي الجيش، لدينا جنودٌ مواطنون يعملون بدوامٍ جزئي في الجيش والبحريّة والقوات الجويّة. أما على الجانب المدني، فلدينا منظمات بيس كوربس وأميريكوربس. وما نحتاج إليه هو منظمة وطنية للدفاع المدني السايبري. ستكون مثل هذه المنظمة شبيهةً بمحاولات الدفاع المدني الأخرى التي شهدها تاريخ البلاد منذ الحرب العالمية الأولى. وبإمكانها اجتذاب الخبراء من جميع أطراف المجتمع بهدف حماية بنانا التحتية المعلوماتية الحساسة من الهجوم، وأمتنا من التهديدات التقانية المتصاعدة القادمة إلينا. ولا بد عندها من إخضاع هؤلاء الأفراد إلى عمليات فحص دقيقة وتقديم تدريب موسّع لهم وإجراء تحقيقات حولهم وتشغيلهم ضمن أطرٌ قانونية وعملياتية معرّفة بدقة. ويبقى التوقيت عاملاً جوهرياً في تأسيس وبناء قوة تعهيدٍ جماهيري تعمل للخير كهذه الآن، وقبل أن تقع الأزمة السايبرية. ثمة الكثير من المنظمات الاحترافيّة في القطاع الخاص قد تكون لها فائدةٌ عظيمة لضمان الزخم في انطلاق مثل هذه المشاريع، كالائتلاف الدولي للشهادات الأمنيّة لنظم المعلومات، وهي منظمة غير ربحية تضم بين أعضائها مئة ألف محترف مُصّدق في الأمن السايبري، جميعهم على أهبة الاستعداد وقادرون على إحداث أثرٍ إيجابي في أيّ مشروع من هذا القبيل إذا ما أرادوا ذلك.

تنهمك شركة الجريمة اليوم في تجنيد أتباعها الذين سيدعمونها في مساعيها. أفليس حرّي بنا أن نقوم بالمثل؟ يمكن للأفراد من جميع الشرائح والخلفيات المساعدة في هذه المشاريع، سواءٌ كانوا من الكبار أم من الصغار، بل حتى من القراصنة الذين يملكون بالتأكيد المهارات المطلوبة لإحداث الفرق لو أنهم رغبوا في توجيه مواهبهم للمصلحة العامّة. وكما

يذكرنا ستيف فوتسنياك، أحد مؤسسي آبل، "لا بأس ببعض التحدي للقواعد". فنحن بحاجةٍ إلى خلق الفرص، خصوصاً بالنسبة للشباب، بما يسمح لهم بحشد مواهبهم وطاقاتهم التي لا يستهان بها لأجل الخير قبل أن تجنّدهم شركة الجريمة في خدمة الشر. فمع الطبيعة الأسّية للتقانة والاستجابة الخطيّة للحكومة سنحتاج إلى أيدٍ أكثر بكثير معنا في المركب تساعدنا على بناء مجتمعٍ آمن ومستقر لن يدمر نفسه. فالأمن العام والسلامة العامة لدينا أهم بكثير من أن نضعها بين أيدي المحترفين لوحدهم. وفي عالم اليوم الذي يتقدم تقدماً أسّياً، في المعركة بين الخير والشر، سيكتب النصر للمجموعة التي تثبت قدرتها على تعبئة الجمهور الأوسع. وقد حان الوقت لإرجاح كفّة هذا النظام لصالحنا لضمان تفعيل أدواتنا التقانية بما يحقق أعظم نفعٍ للبشرية في المحصلة.

تلعيب النظام

على كل مصمم ألعاب أن يطوّر لعبةً واحدةً تغير العالم تغييراً واضحاً. فإذا كان المحامون يقومون بالعمل التطوعي، فلماذا لا نقوم بذلك نحن أيضاً؟

جين مك. غونيغال

وفقاً لمصمم الألعاب الأميركي والباحث جين مك.غونيغال، ثمة اليوم أكثر من نصف مليار شخص في العالم يلعب ألعاب الحاسب والفيديو لساعةٍ واحدةٍ في اليوم على الأقل، منهم أكثر 183 مليون شخص في الولايات المتحدة لوحدها. ويصل المجموع إلى ثلاثة مليارات ساعة في الأسبوع تُمضى على مستوى الكوكب في ألعاب الفيديو. فماذا لو أمكن توجيه هذه الجهود لتحقيق منافع عامة معينة؟ تخيل الطاقة الهائلة والإمكانات التي سيمكن عندها أن تنطلق. من شأن ذلك أن يجمع حكمة الجماهير بما يسمح بالتعامل مع بعض أكبر التحديات التي يواجهها العالم. ولاختبار هذه

النظرية طورت داربا عام 2009 تحديًّا شبكياً (يعرف أيضاً بتحدي البالون الأحمر)، حين خبأت عشرة بالونات هليوم حمراء في أماكن عامة في أنحاء الولايات المتحدة في مدنٍ من ميامي إلى بورتلاند، وعرضت 40 ألف دولار جائزةً للفريق الذي يعثر على جميع البالونات أولاً. وقد خرجت داربا بهذه المنافسة لاستكشاف الدور الذي قد يؤديه الإنترنت والشبكات الاجتماعية في الاتصالات بالزمن الحقيقي والتعاون على مسافات كبيرة، بهدف حل مشكلات يمثل الزمن فيها عاملاً حرجاً، كعمليات الإغاثة بعد الكوارث في أوقات الأزمات. ومن اللافت أن فريقاً من معهد ماساتشوستش للتقانة، استطاع العثور على جميع البالونات العشرة المخبأة في أقاصي البلاد خلال تسع ساعاتٍ فقط، عبر التعهيد الجماهيري للمهمة من خلال الوسائط الاجتماعية وإيكالها إلى 4400 متطوع.

سرعان ما يتبين أن لعب الألعاب ليس بالضرورة مضيعةً للوقت، بل يمكنه في الحقيقة أن يتحول إلى فعاليةٍ ذات إنتاجيةٍ عالية. والتلعيب هو حقل دراسةٍ جديد يسمح باستخدام طرق التفكير وآليات اللعب واستغلالها في سياقات لا علاقة لها باللعب، عبر تشجيع اللاعبين وإشراكهم في حلّ مشكلات العالم الحقيقي الفعليّة. ومن الأمثلة على ذلك عمليات التشخيص والمعالجة للملاريا في مجال الصحّة العامة. فعلى مستوى العالم، توجد أكثر من 600 ألف حالة إصابة بالملاريا كل يوم تنتج عنها وفاة طفل كل دقيقة. وينتشر هذا المرض بلدغات البعوض التي تنقل الطفيليات إلى جسم الإنسان وتصيب خلايا الدم الحمراء لدينا. وتشخيص الملاريا عملية تستغرق وقتاً طويلاً وتحتاج إلى ثلاثين دقيقة يمضيها متخصص في البحث يدوياً عن الطفيليات في الدم تحت المجهر، ليبقى كثير من المصابين بلا تشخيص ليس أمامهم سوى الموت. لكن لعبة مالارياسبوت تهدف إلى تغيير ذلك عبر استخدام صورٍ افتراضية من شرائح دم تعود إلى مرضى فعليين

وتقديمها إلى اللاعبين، متحديةً إياهم أن يجدوا ويسموا أكبر عددٍ ممكن من الطفيليات خلال دقيقةٍ واحدة. وكانت النتائج مثيرةً للإعجاب، فخلال شهرٍ واحد لعب لاعبون مغْفلو الهوية من 95 بلداً 12 ألف لعبة. فبعد تلقي تدريبٍ على الإنترنت لا يستغرق سوى بضع دقائق يشرح للاعبين أشكال الطفيليات، تمكن لاعبو ملارياسبوت من التعرف بدقة على أكثر من 700 ألف طفيلي. وبفضل عرض الصورة نفسها على عدة لاعبين، حقق هؤلاء اللاعبون الذين لا يملكون أي خبرة طبيّة معدل دقة تجاوز 99 بالمئة، وهو إنجازٌ قادرٌ على "تغيير قواعد اللعبة" في عالم معالجة الملاريا وتشخيصها. وفي حالةٍ أخرى، تسمح لعبةٌ تسمّى "فولد إت" للاعبيها الذين لم يخضعوا لتدريبٍ خاص في البيولوجيا الجزيئية بحلّ الأحجيات لصالح العلم، باستخدام مهاراتهم في التوجه الفراغي الثلاثي الأبعاد لمعالجة وفضّ جزيئات بروتينية كطريقةٍ لدراسة الأمراض ومعالجتها. وفي إحدى الوقائع اللافتة، تمكن لاعبوا فولد إت بدقة من التعرف على بنية إنزيمٍ يؤدي دوراً حاسماً في تكاثر فيروس الإيدز خلال بضعة أيامٍ فقط، وهو اكتشافٌ عجز عنه باحثو الإيدز في أنحاء العالم الذين كانوا يحاولون حلّ المشكلة بأنفسهم على مدى أكثر من عقد.

يمكننا استقاء دروسٍ هامة من ألعاب التعهيد الجماهيري الملهمة إلى حدٍّ بعيد مثل ملارياسبوت وفولد إت، ويمكننا تطبيق ما تعلمناه في حلّ الألغاز التي تواجهنا في ما يتعلق بانعدام الأمن التقاني لدينا. فأيّة ألغازٍ ممتعة يمكننا أن نطور لكي نزيد من مشاركة العامة، وخصوصاً الشباب منهم، لكي نوظف حبهم للعب بغرض تحسين أمننا السايبري؟ تخيل الإمكانات المتاحة. فبدلاً من عرض صور شرائح الدم للبحث عن إصابات الملاريا، يمكننا تقديم رسائل تصّيد بالبريد الإلكتروني بالزمن الحقيقي لنطلب من الجمهور تحديد الرسائل الخبيثة التي تطلب معلومات الحساب المصرفي بدقة، مع

منح نقاطٍ وجوائز لأفضل اللاعبين. قد يساعد تلعيب عملية تأمين البرمجيات شركات التقانة على تجنب الأخطاء الواضحة الناتجة عن عقلية "سلّم وحسب"، عبر حشد عشرات الآلاف من اللاعبين حول العالم وإرسالهم في رحلة "صيد حشرات"، يبحثون خلالها عن الثغرات في المنتجات البرمجية والعتادية هذه، تلك الثغرات التي كان يمكن لشركة الجريمة وقراصنتها أن تستغلها لإلحاق الضرر بالناس. وهذه الفكرة قيد التطوير بالفعل لدى داربا، إضافةً إلى العديد من الشركات الناشئة، مثل توب كودر وبَغ كراود، بل يمكن تطبيق هذه التقنيات كما هي على نظم البنى التحتيّة الهامة في البلاد أيضاً. حيث يمكن عرض بيانات مغفلة الهوية على اللاعبين على طراز اللعبة الإحيائيّة سيم سيتي، وتركهم يبحثون عن نقاط الضعف الأمنيّة في كل شيء، من شبكات الكهرباء الافتراضيّة لدينا إلى شبكات النقل. وقد ينجح اللاعبون الأفراد في النهاية في تحقيق قفزاتٍ كبيرة في مجال الأمن السايبري دون أن يكون لديهم أي سببٍ لفعل ذلك سوى الاستمتاع باللعبة. لكن آخرين ستدفعهم القدرة على حل مشكلات العالم الحقيقي ومساعدة الآخرين، أما بالنسبة لأولئك الذين لا يجذبهم هذا ولا ذاك، فثمة دائماً الجوائز النقدية.

عينٌ على الجائزة: المنافسات المحفّزة للأمن العالمي

إلى أن يُكتشف أنه فتحٌ حقيقي، يبقى كل شيء فكرة مجنونة.

بيتر ديامانديس

الجوائز هي طريقة لاجتذاب تركيز الدماغ. وما عليك سوى أن تسأل الحشود التي تجرّب حظها مع الجائزة الكبرى ليانصيب ميغامليونز. لكن الجوائز قد تكون أيضاً الشرارة التي توصل إلى حلّ ثوري لمشكلةٍ عويصة. وهو ما حدث عندما أسّس البرلمان البريطاني جائزة لونغتيود عام 1714، سعياً منه لدعم الملاحة البحرية لضمان "أمن وسرعة الرحلات، وحفظ

السفن، وحياة البشر". فمع أن خط العرض (أي الموضع بين الشمال والجنوب) كان سهل القياس بالاعتماد على موقع الشمس، فإنّه حتى بداية القرن الثامن عشر لم تكن هناك وسيلةٌ لدى البحارة لحساب موقعهم وفقاً لخطوط الطول من الشرق إلى الغرب. وعبر القانون الذي وضعه البرلمان، قدمت الحكومة البريطانية 20 ألف جنيه استرليني (أي أكثر من مليون جنيه استرليني اليوم) للحلّ الذي يستطيع حساب خط الطول في نطاق نصف درجة. وألهمت الجائزة المحفّزة جون هاريسون، وهو صانع ساعات من الطبقة العاملة لديه القليل من التعليم الرسمي، باختراع الميقات البحري، وهو جهازٌ شبيهٌ بالساعة يحلّ المشكلة. وبعد مضي مئتي عام على ذلك، أطلقت جائزةٌ محفّزة أخرى، هذه المرة لحفز التطورات في حقل الطيران الناشئ.

أصبح تشارلز ليندبرغ أول رجلٍ يحلّق فوق الأطلسي، لا نتيجة حسّ المغامرة لديه، بل لأنّ قطب الأعمال الفندقية الذي قلما يُذكر ريموند أورتيغ عرض 25 ألف دولار من ماله الخاص عام 1919، جائزةً لـ "أول طيّار من أي بلد حليف يعبر الأطلسي برحلة طيرانٍ واحدة من باريس إلى نيويورك أو من نيويورك إلى باريس". لقد قدم أروتيغ الجائزة التي ستدفع قدماً تقانةً جديدةً موجودةً في أيامه هي الآلة الطائرة. ولم تتلق المحاولة تمويلاً من الحكومة، كما لم يكن هناك ربحٌ مباشر يمكن تحقيقه، لكن ذلك لم يمنع تسعة فرق مستقلة من إنفاق نحو 400 ألف دولار سعياً وراء جائزة الـ 25 ألف دولار. لقد كانت الجائزة بمثابة الشعلة الأساسية، ذلك الشيء الذي أطلق شرارة الإبداع الذي حلّ المشكلة وساعد في خلق صناعة الطيران التي نعرفها اليوم. وفي عام 1996 ارتدى بيتر ديامانديس، الطبيب المتحمّس للفضاء والمتعهد المتسلسل، رداء أورتيك وأسّس مؤسّسة إكسبرايس، وهي منظمةٌ غير ربحيّة تعمل على تصميم المنافسات العامة وإدارتها بهدف

تشجيع التقدم التقاني لتحسين حياة الجنس البشري. فربما حان الوقت لمثل هذه المنافسات في مجال الأمن السايبري.

يرى دياماندیس أن "إكسبرايس هي جائزةٌ مرموقة ومحفّزة تهدف إلى توسيع حدود الممكن لتغيير العالم نحو الأفضل. إنها تحصد خيال العالم وتلهم الآخرين بالوصول إلى أهدافٍ مشابهة ما يحفّز الإبداع ويسرّع معدل التغيير الإيجابي". وكانت أول جائزة يعلنها دياماندیس على الإطلاق هي جائزة إكسبرايس أنساري البالغة قيمتها عشرة ملايين دولار، كان التحدي فيها هو إطلاق سفينة فضائية مأهولة تمّر بخط كارمان (على ارتفاع 100 كلم) قبل أن تعود إلى الأرض بسلام. وكأن ذلك لم يكن كافياً، فقد كانت قواعد المنافسة تنصّ على أن السفينة الفضائية يجب أن تتمكن من حمل وزن شخصين بالغين إضافيين، وأن تقوم بعملية إطلاقٍ ثانية خلال مدة أسبوعين. ومن دون أي دعمٍ حكومي قام 26 فريقاً بإنفاق ما يصل إلى مئة مليون دولار سعياً للوصول إلى الهدف السامي، وفي خريف عام 2004 نجح فريق موجيف لمشاريع صناعة الفضاء في إنجاز ما قد يمهّد الطريق لسياحة الفضاء وغيرها من الرحلات الفضائية التجاريّة. تتميز الجوائز المحفّزة بالجرأة والشجاعة، وهي تستقطب اهتمام العالم، وهو بالذات نوع التفكير الذي نحتاج إليه لكي نحقق قفزةً كبيرةً نحو حماية أنفسنا من المخاطر التقانية العميقة التي نواجهها اليوم.

من شأن جائزة إكسبرايس مخصّصة لمجال الأمن السايبري، أن تكون محركاً للإبداع وحافزاً مدهشاً يدفع بالتغيير الأسّي نحو الخير ويعالج مشكلة انعدام الأمن التقاني في العالم بما يعود بالنفع على البشرية كلها. فعبر تعريف المشاكل الأمنيّة السايبرية التي نعانيها بوضوح، تستطيع الجائزة أن تحفز الفرق من أنحاء العالم إلى التوصل إلى حلولٍ فعالة بطريقة ربما تضمن تجنب الأزمات، بينما تزيد الناس قوة وتولد تقاناتٍ

جديدة، بل وربما تخلق صناعاتٍ جديدة. وربما تساعدنا مثل هذه الجائزة في مجال الأمن السايبري على التغلب على أحد أعظم التحديات التي نواجهها في ما يتعلق بالمخاطر القادمة من التقانات الأسّية، وهو الاعتقاد بأن هذه المشاكل غير قابلة للمعالجة والحل وأنه ما من طريقٍ واضح يقود إلى الحل. لقد سبق لنا أن مررنا بأوقاتٍ عصيبة، وتمكّن نوعنا عدة مراتٍ من تحقيق أشياء كانت تبدو ذلك قبل ذلك بيومٍ واحد وكأنها أفكارٌ مجنونة. تلهم الجوائز المحفّزة الأمل عبر رؤيا المستقبل الأفضل، وأولئك الذين يفوزون بهذه الجوائز يثبتون أن بعض مشكلاتنا التي تبدو عصيةً على الحل هي قابلةٌ للحل، بل وستحلّ أيضاً. وفردٌ واحد أو فريقٌ صغير قادرٌ بالتأكيد على إحداث فرق، كما بين ليندبرغ وهاريسون وآخرون كثيرون. والأهم من ذلك هو أن جائزة أكسبرايس في مجال الأمن السايبري ربما لا تكون سوى البداية في تحقيق تقدماتٍ كبيرة في مجال الأمن العالمي. والتهديدات الأخرى الناشئة مثل الإرهاب البيولوجي وخروج الذكاء الصنعي عن السيطرة وأنظمة الأسلحة المستقلة ذاتياً وتقانة النانو، باتت بدورها ناضجةً بما يكفي لاستغلال الجوائز التحفيزية، خصوصاً إذا ما نظرنا إلى حجم المجازفة الوجودية التي تفرضها على العالم.

تماماً كما حفّز فاعل الخير ريموند إرتيك الملاحة الجوية المدنية وأعطى أنوشيه وأمير أنصاري الدفع لصناعة الفضاء التجارية، يمكن لفاعلي الخير اليوم أن يحدثوا فرقاً كبيراً في مجال الأمن التقاني. ولنا مثالٌ في الأعمال البطولية المدهشة التي حققتها مؤسسة بيل وميليندا غيتس في مكافحة الإيدز والقضاء على شلل الأطفال ودعم التعليم، عبر توزيع مبلغٍ مدهش بلغ 26 مليار دولار من ثروة السيد غيتس منذ تأسيس المنظمة. لكنهم ليسوا الوحيدين في هذا المضمار، إذ يوجد بالفعل نوعٌ جديد من "فاعلي الخير التقانيين" الملتزمين باستخدام ثرواتهم لتحسين العالم. فالرئيس الأول

لموقع إيباي جيف سكول، يعمل بلا كللٍ لمحاربة الأوبئة والحد من الانتشار النووي، مانحاً منظمته نحو المليار دولار من ماله الخاص. وقد قام إيلون مَسك وبيير أوميديار وباول ألين وستيف كيس ولاري إيليسون ومو ابراهيم والسير ريتشارد برانسون وميشيل لبومبيرغ جمعياً بتوقيع "عهد المنح"، السخيّ إلى حدٍّ لا يصّدق، ملتزمين بتخصيص جلّ ثرواتهم للأعمال الخيرية. فلدى هؤلاء الأفراد شغفٌ شخصي يدفعهم إلى دعم نشاطاتٍ تتنوع، من تحسين الحكومات إلى تطور الطفل، بثرواتهم بتفاني. ونظراً لكون معظم هؤلاء قد جنوا ثرواتهم، كلها أو جزءاً منها، عبر العمل في مجال التقانة، فإن تمويل جائزة أكسبرايس تركز على هذا الموضوع، قد يحقق خطواتٍ كبيرة في مواجهة التحديات التقنية التي تظهر أمامنا بما يحدث فرقاً هائلاً، خصوصاً إذا ما نظرنا إلى خبرتهم في هذا المجال. ومن المفرح أن منظمة إكسبرايس هي اليوم في المراحل الأولى لدراسة تأسيس جائزةٍ في مجال الأمن السايبري مع دعمٍ من مؤسسة دلويت الاستشارية. وستكفي دفعةٌ من 20 مليون دولار فقط (أي ما لا يتعدى 0.01 بالمئة من العوائد السنوية للمليارات الـ 150 التي تحققها صناعة البرمجيات)، لقطع شوطٍ طويل نحو تأمين برمجياتٍ أكثر استقراراً وأمناً لا بدّ منها لحماية مستقبلنا التقاني. إلا أنه من الممكن تحقيق المزيد بعد، إذ يمكن تحقيق شيءٍ كبير وجريء يوازي في أبعاده التحديات التقانية التي تضغط علينا اليوم.

البدء بالجد: مشروع مانهاتن للفضاء السايبري

> خلال مشاركتي في مشروع مانهاتن وأبحاثي اللاحقة في لوس ألاموس على مدى خمسة عشر عاماً، كنت أعمل برفقة ما كانت ربما أعظم مجموعةٍ من المواهب العلمية يشهدها العالم على الإطلاق.
>
> فريدريك رنز

حين تم اكتشاف توصل الفيزيائيين الألمان إلى طريقة شطر ذرة اليورانيوم

عام 1939، انتشرت المخاوف بسرعة عبر الأوساط العلمية الأميركية، من أن النازيين سيتمكنون قريباً من تطويرٍ قنبلةٍ قادرةٍ على نشر قدرٍ من الدمار لا يمكن تخيله. وقد اتفق ألبرت أينشتاين وإنريكو فيرمي على أنه لا بد من إبلاغ الرئيس فرانكلين ديلانو روزفلت بالمستجدات. وبعد ذلك بوقتٍ قصير أطلق مشروع مانهاتن، وهو مشروعٌ سرّي ملحمي للحلفاء خلال الحرب العالمية الثانية يطمح لبناء سلاحٍ نووي. فأعدت المرافق في لوس ألاموس ونيومكسيكو وعُيّن روبرت أوبنهايمر ليشرف على المشروع. وبين عامي 1942 و1946 شغل مشروع مانهاتن سرًّا أكثر من 120 ألف أميركي كانوا يعملون بلا كللٍ على مدار الساعة في أنحاء البلاد بكلفةٍ بلغت ملياري دولار. لقد كان أولئك العاملون في مشروع مانهاتن جادين تماماً حيال التهديد الذي يحيق بهم. أما نحن فلسنا كذلك.

ربما لن يقدم شخصٌ عاقل على مساواة المخاطر التي يفرضها الأثر الكارثي لحربٍ نووية بتلك الناجمة عن سرقة 100 مليون بطاقة ائتمانية، لكن بعض الاكتشافات العلمية الجارية اليوم، بما فيها الذكاء الصنعي وتقانة النانو والبيولوجية التركيبية، قد تمثل بالفعل تهديداً هائلاً للحياة على هذا الكوكب، كما يحذّر ستيفن هاوكينغ وأيلون موسك وآخرون. وبعيداً من هذه التهديدات الوجودية المحتملة، يمكننا بلا شك أن ندرك أن الأسس التي يقوم عليها مجتمعنا التقاني الحديث، والمتمثلة في البنى التحتية الحساسة العالمية، ضعيفةٌ ومهددةٌ بالانهيار إما عبر البنى المتقادمة المتهالكة، أو عبر التعقيد القاهر للنظام أو الهجوم المباشر من قبل أطراف خبيثة.

إذا كنا نعلم أننا سنعاني حين يقع الهجوم السايبري المفجع الذي سيغير قواعد اللعبة كما تم تحذيرنا، فماذا ننتظر حتى يحدث ذلك لكي نتحّضر؟ إن الأدلة على المخاطر التقانية من حولنا جليّة. ففي كل يوم تعرقل

الهجمات السايبرية نظامنا المالي ويسرق اللصوص المليارات على شكل ملكية فكرية، وتنهب الحكومات الأجنبية تصاميم أسلحتنا العسكرية ويتبادل القراصنة الإرشادات في ما بينهم حول السيطرة على نظم التحكم الصناعي التي تشغّل كل شيء، من محطات الطاقة إلى مرافق المياه والصرف الصحي. تحضرني هنا مقولة الإحصائي المعروف ومحرّر مدونة 538 نيت سيلفر، بأن أسلوبنا المتكاسل لحل مشكلة الأمن السايبري ونقاط الضعف التقانية العميقة التي نعانيها لا تزال حتى اليوم أشبه باستخدام واقٍ شمسي والادعاء بأنه يحمينا من انصهارٍ نووي، فهو غير ملائم أبداً لحلّ مشكلةٍ بهذه الأبعاد. لقد آن أوان إعادة التفكير على نحوٍ بارد ومتشائم بالحال التي آلت إليها حياتنا. لقد حان وقت مشروع مانهاتن في مجال الأمن السايبري.

لست أنا أول من يقترح مثل المبادرة، فقد فعل كثيرون ذلك من قبل، وخصوصاً في أعقاب هجمات الحادي عشر من أيلول. ففي ذلك الحين، كتب لفيفٌ من العلماء البارزين إلى الرئيس جورج دبليو.بوش رسالةً حذروه فيها من أنّ "البنى التحتية الحساسة في الولايات المتحدة، بما فيها الطاقة الكهربائية والمالية والاتصالات والرعاية الصحية والنقل والماء والدفاع والإنترنت، ضعيفةٌ جداً أمام الهجمات السايبرية. ولا بد من اتخاذ تدابير حازمة تخفف وطأة المشكلة لتجنب كارثةٍ على مستوى البلاد. وكان من بين الموقعين على العريضة أكاديميون وبيوت خبرة وشركات تقانة ووكالات حكومية، منها مديرون سابقون لداربا وإدارة الاستخبارات الأميركية وهيئة العلم الدفاعي وكزيروكس بارك، والعديد من المختبرات الوطنية وجامعة رابطة اللبلاب. حيث حذر هؤلاء المفكرون الجادون، الذين لا يميلون إلى الغلو والمبالغة، من أن التهديد الكبير الذي يفرضه هجومٌ سايبري هو خطر حقيقي وحاضر، وطالبوا الرئيس بالتصرف فوراً عبر إطلاق مشروع دفاع

سايبري على غرار مشروع مانهاتن. كان ذلك النداء عام 2002. إلا أن القليل الثمين قد تغير منذ ذلك الوقت للأسف في حالة انعدام الأمن السايبري في العالم. وإذا كان ثمة تغيير أساساً، فإن الأمور قد ساءت. ولا شك في أن جهوداً شكليةً قد بذلت، وأنّ الكراسيّ قد أعيد ترتيبها على ظهر سفينة التايتانيك، لكن لم يفعل الكثير لتحقيق تقدمٍ جوهري. فما هي استراتيجية أميركا الشاملة حيال التهديدات التقانية الناشئة السريعة النمو التي نواجهها؟ ليست لدينا أية استراتيجية ببساطة، وهي مشكلةٌ خطيرة ربما نندم عليها ذات يوم.

من شأن مشروع مانهاتن حقيقي يكّرس للفضاء السايبري أن يجمع بعض أعظم أدمغة زماننا، من الحكومة والأكاديميا والقطاع الخاص والمجتمع المدني. ويمكن للحكومة، التي ستؤدي دور المشرف والممول، أن تجمع أفضل وألمع علماء الحاسب والمتعهدين والقراصنة وهيئات البيانات الكبيرة والباحثين العلميين وأصحاب رأس المال المغامر، والمحامين والخبراء في السياسة العامة وضباط السلطة التنفيذية، والمسؤولين عن الصحة العامة إضافةً إلى الكوادر العسكرية والاستخبارية. وسيكون هدفهم هو خلق قدرات دفاع سايبري وطنية حقيقية، تستطيع اكتشاف التهديدات التي تحيق ببنانا التحتية الوطنية الحساسة بالزمن الحقيقي وتستجيب إليها. سيساعد مشروع مانهاتن هذا على التوصل إلى الأدوات ذات الصلة التي تحتاج إليها لحماية أنفسنا بما فيها نظم التشغيل المستقرة الآمنة ذات الخصوصية المحسّنة. ومن خلال الأبحاث التي تجري في إطاره، سيسمح المشروع بتصميم وإنتاج برمجياتٍ وتجهيزاتٍ قادرةٍ على معالجة نفسها وتمتاز بقدرةٍ أكبر على مقاومة الهجمات وتتميز بالمرونة في الاستجابة إلى الإخفاقات أكثر من أي شيءٍ نعرفه اليوم. وسيكون لهذا المشروع ذي الأهمية القومية، بل العالمية، رؤياه ومداه وموارده وميزانيته التي ستضمن

نجاحه. والأهم من ذلك هو أن المشروع سيتطلب الإحساس بإلحاح المشكلة على غرار مشروع مانهاتن الأصلي، وهو ما يغيب حتى الآن كلياً في مساعينا الحالية والسابقة المتعثرة للتصدي لحالة انعدام الأمن المتنامية لدينا.

ربما تبدو مثل هذه المهمة مهيبةً، لكن ثمة أخبارٌ طيبة. فنحن قادرون على القيام بذلك. يمكننا كسب هذا الصراع. نحن كشعب يتوفر لدينا بلا شك ما يتطلبه إحداث تغييرٍ عميق في أمننا المشترك يدفعه نحو الأمام. فذلك يتطلب رؤيا وتركيزاً وقيادة. وإذا كان الأمر يبدو محبطاً في بعض الأحيان، فلنستلهم بعض التشجيع من الرئيس جون إف.كينيدي، الذي استطاع في خطابٍ له في جامعة رايس في أيلول عام 1962 إقناع الشعب الأميركي بتمويل ناسا لتصل بالإنسان، قبل نهاية ذلك العقد، إلى القمر وتعيده سالماً إلى الأرض. ففي خطابه البليغ المحمّس أمام 35 ألف متفرج، مجّد السفر عبر الفضاء كجزءٍ لا يتجزأ من أمننا العالمي منوهاً إلى أنّ:

> الإنسان، في سعيه وراء المعرفة والتقدم، عاقد العزم لا يستطيع أن يتردد... لقد أقسمنا أن لا نسمح برؤية الفضاء يتحول إلى مكانٍ يعجّ بأسلحة الدمار الشامل، بل بأدوات العمل والفهم... ونحن إذ نبحر في عباب هذا البحر الجديد فإنما لوجود معرفةٍ جديدة يمكننا اكتسابها وحقوقٍ جديدة نحصّلها، وهي لا بد من تحصيلها وتسخيرها لتقدم جميع البشر. فعلم الفضاء، على غرار العلم النووي والتكنولوجيا عموماً، ليس لديه ضميرٌ بحد ذاته. والإنسان هو الذي يقرر ما إذا كان هذا العلم سيكون أداة خير أم أداة شر. نحن حين نختار الذهاب إلى القمر خلال هذا العقد والقيام بالأشياء الأخرى، ليس لأنها سهلة، بل لأنها صعبة، لأن هذا

> الهدف سيساعد على تنظيم وقياس أفضل طاقاتنا ومهاراتنا، ولأننا نقبل بهذا التحدي، هذا التحدي الذي لا نريد تأجيله، هذا التحدي الذي نريد أن نكسبه... ونحن لهذا إذ نبحر، نطلب بركة الله في أعظم المغامرات التي يتجرأ عليها الإنسان على الإطلاق وأكثرها مجازفةً وخطراً.

أجل، هذا ما كنت أتحدث عنه. أين هو ذلك القائد؟ ذلك الرجل أو تلك المرأة، ذلك الشخص الذي سيأخذنا بشجاعةٍ في القرن الحادي والعشرين فيسخّر تقاناتنا من أجل خيرنا المشترك، ويكون مستعداً للمجازفة بسمعته وشرفه للقيام بهذه المهمة المقدّسة مظهراً الشجاعة والعزم والإيمان الراسخ الذي يتطلبه تحقيق هذا الهدف. فقط عبر التنسيق المحموم بين جهود الحكومة والأكاديميا والقطاع الخاص سنحقق التقدم. والمفتاح لجعل مشروع مانهاتن المخصص للفضاء السايبري ينجح بالفعل، هو الحسّ الأصيل بالجديّة وبحجم وأهمية المهمة التي أمامنا. فالساعة تدق وما من وقتٍ أفضل من اليوم الحاضر لجعل هذه الفكرة تثمر.

أفكار أخيرة

> أفضل طريقةٍ للتنبؤ بالمستقبل هي اختراعه.
>
> ألان بايك، كزيروكس بارك

في ما يتعلق بالتهديدات التقانية التي تستهدف مجتمعنا، يمكننا القول إن المستقبل قد صار بالفعل هنا. فهو يجلس في بناءٍ للمكاتب في كييف معَداً لأن يكون شركة إنّوفيتف ماركتنغ القادمة. وهو يقبع في الحاسب المحمول لذلك الصبي الذي يجلس إلى جانبك في المكتبة العامة يعمل على بناء طريق الحرير التالي وسوق الاغتيال القادمة. إنّه في البناء الحكومي المؤلف من عشرة طوابق في تلك العاصمة الأجنبية البعيدة، حيث يذهب آلاف الجواسيس الرقميين للعمل كل يوم محاولين سرقة أسرارك التجارية.

إنه في مرآب ذلك القرصان البيولوجي الغاضب، الذي سَئم التنمر في المدرسة ويخطط الآن لثأره الإرهابي البيولوجي. إنه في ذلك المتجر المحلي الذي يبيع المروحيات المسيّرة دون أن يعلم ما إذا كانت ستستخدم لنقل الأسلحة من فوق أسوار سجنٍ أو مطار. وهو متوفر عبر موقع الويب الذي يبيع نماذج لطائراتٍ نفاثة قادرة على الطيران بشكلٍ مستقل، محملة بالمتفجرات ليوجهها الإرهابيون نحو بناءٍ مكتظ. لقد وصل هذا المستقبل بالفعل. وجميع التحذيرات والمؤشرات باتت موجودة. والتهديد القائم خطير، وقد حان وقت التحضر له الآن. ويمكنني أن أؤكد لك أن المجرمين والإرهابيين وغيرهم من الفاعلين الخبثاء قد قاموا بالتحضر منذ اليوم.

كما رأينا، فإن كل شيءٍ متصل وما من أحد حصين. لكننا لم نخسر كل شيءٍ بعد، وثمة أشياء يمكننا فعلها حيال ذلك كما لخصنا في هذا الفصل وفي الفصل الذي سبقه. لكننا حين نفشل في الاستجابة لهذه المشكلة التي بين يدينا وندفن كالنعامة رؤوسنا في الرمال، فإن المشكلة لن تحلّ نفسها، بل ستنمو. والتحديات التي نواجهها كبيرةٌ وفي تعاظم. والأمر لا يتعلق فقط بحساباتٍ مصرفية يتم اختراقها أو بصورٍ شخصية تتم سرقتها. كما لا يتعلق بمجرد الحفاظ على خصوصيتنا وتمكين سيطرتنا على طيفٍ واسع من الأجهزة التي دخلت حياتنا. بل يتعلق بحراسة مستقبلنا التقاني وفهم ما هو قادم. وكما يذكرنا مارشال ماك.لوان "إن الإطار أيضاً يتغير مع كل تقانةٍ جديدة لا فقط الصورة التي في الإطار".

ستؤثر اختراقات الغد على سياراتنا وعلى نظم المواقع الجغرافية والأجهزة الطبية المزروعة وأجهزة التلفاز والمصاعد والعدادات الذكية وأجهزة مراقبة الأطفال وخطوط التجميع، ومع 79 أوكتلوين اتصال جديد سيصبح ممكناً بفضل الإصدار السادس من بروتوكول الإنترنت وإنترنت الأشياء، ستصبح جميع الأغراض المادية قابلةً للاختراق، بما فيها جميع الشاشات التي تسود

حياتنا. لكننا حتى يومنا هذا لا نمتلك أية نماذج قابلة للاستمرار لحوسبةٍ آمنة وموثوقة بحق، وهو فشلٌ حقيقي بالنسبة لمجتمعٍ مبني على الحواسب ويتم تشغيله بواسطتها. وليست لدينا طريقة مجرَّبة تسمح لنا بالوثوق من الشيفرات البرمجية التي تدير حياتنا وعالمنا. وهو ما يسمح لأولئك الذين يتحكمون بالشيفرة البرمجية بالسيطرة على عالمنا، سواءٌ للخير أم للشر. وبعيداً من ذلك، سيترتب علينا التعامل مع أسلحة بيولوجية وعمليات اختراق تستهدف الـ دي.إن.إي وعمليات انتحال جيني وبيومتري للهوية، ناهيك بالخوارزميات الجاهزة التي يسهل التلاعب بها وأنظمة الذكاء الصنعي. نحن نعيش أوقاتاً أسّية، وعلى الرغم من أنه يسهل استبعاد أفكار الروبوتات القاتلة المستقلة والذكاء الصنعي الشرير الأشبه بما نشاهده في سكاينت، واعتبار كل ذلك مجرد خيالٍ علمي حول المستقبل، فإن جورج كارلن يذكرنا بأن "المستقبل سيصبح قريباً جزءاً من الماضي".

في عالم تدير فيه الحاسب جميع نظمنا وبنانا التحتية الهامة، سيكون من السهل الاستهانة بمسألة الغياب المزمن للأمن التقاني واعتبارها مشكلة متعلقة بالحواسب. لكن ما لدينا ليس مجرد مشكلة متعلقة بتقانة المعلومات. فتشابك التقانة مع كامل نسيج الحياة الحديثة يجعل المشكلة اجتماعية وشخصية ومالية، ومتعلقة بالرعاية الصحية والحكومة والحكم والتصنيع والسلامة العامة والنقل والطاقة والخصوصية وحقوق الإنسان. وما من خيار أمامنا سوى أن نكسب المعركة الدائرة لربح أرواح تقاناتنا لأن البدائل، إذا أردنا الصراحة، أفظع من أن نفكر فيها. يجب أن يكون هذا نداءً لنا لنتحرك.

لذا، فقد حان الوقت لإعادة تقييم ما كنا نعتبره بديهياً في هذا العالم التقاني الحديث تقييماً كاملاً، ولوضع اتكالنا على آلات كلية الوجود لا

تفهمها سوى قلة قليلة موضع تساؤل. ونحن لا نقوم بذلك نتيجة رهابٍ أعمى من التقانة ولا دفاعاً عن أسلاف محطمي الآلات، بل كإجراءٍ ينسجم مع الحسّ العام مع التقدير الكامل للإيجابيات الكبيرة التي ستصبح ممكنة بفضل هذه التقانات الأسّية. لا يمكن وقف الإبداع، والتغييرات التقانية تأتي بسرعةٍ متزايدة. لقد وصلنا إلى نقطة الانقلاب، تلك اللحظة الزمنية التي تتطلب تركيزنا الفوري بأقصى قدرٍ ممكن. فاليوم التاسع والعشرون للزنبقة المائية في المستنقع يقترب بسرعة، وكما يحدث مع جميع الأشياء الأسّية، فإن المجال المتاح أمامنا للتصرف على نحوٍ مسؤول وفعال ينحسر بسرعة. ثمة طريق مفتوحةٌ إلى الأمام تبعدنا عن التهديدات التقانية التي نواجهها اليوم. فمن خلال تعبئة المواطنين العاديين واستعادة سيطرتنا على أجهزتنا وآلاتنا، يمكننا جميعاً استغلال هذه الأدوات لتحقيق أكبر منفعةٍ ممكنة. بعبارةٍ أخرى فإن الأدوات الكفيلة بتغيير العالم موجودةٌ بين يدي كل شخص. أما كيفية استخدامنا لها فلست أنا من يقررها بل نقررها جمعياً. والمستقبل الأفضل الذي نصبو إليه لن يظهر بسحر ساحر من تلقاء نفسه. بل سيتطلب انتباهاً هائلاً وجهوداً جبارة ونضالاً طويلاً. لكن مع هذ العمل المضني، لن نتمكن فقط من النجاة عبر هذا التقدم، بل من الازدهار إلى حدٍّ لم نكن لنتخيله من قبل. هذا هو العالم الذي أريد أن أعيش فيه.

انتهى